

Overvågning, privatliv og sikkerhed

HVAD MENER DU?

1 Velkommen til SurPRISE

Velkommen til det europæiske forskningsprojekt SurPRISE. SurPRISE er en forkortelse for 'Surveillance, Privacy and Security' (Overvågning, Privatliv og Sikkerhed). Formålet er at høre borgernes holdninger til nye sikkerhedsteknologier. Mange af disse teknologier benytter sig af overvågning af mennesker og deres adfærd. Poliiti og andet sikkerhedspersonel bruger teknologierne til at kontrollere, hvad der foregår i det offentlige rum. Når du tager ud i lufthavnen, og din bagage bliver tjekket af scanningsudstyr, eller når et overvågningskamera filmer, hvad der foregår på gader og stræder, er du udsat for overvågningsbaserede sikkerhedsteknologier. Formålet med SurPRISE er at bidrage til, at disse teknologier er effektive, sikre og respekterer menneskerettighederne. For at kunne indfri målet har vi brug for din hjælp.

Vi har inviteret dig til at deltage i SurPRISE projektet, fordi EU-Kommissionen ønsker at finde ud af, hvad der kan gøres for at få borgerne til at føle sig sikre og trygge. Når du deltager i SurPRISE borgertopmødet, kan du dele dit syn på de nye sikkerhedsteknologier med dine medborgere. SurPRISE vil samle borgernes synspunkter på de nye sikkerhedsteknologier og videreformidle dem til EU-Kommissionen.

Der afholdes borgertopmøder i ni europæiske lande – Danmark, England, Østrig, Tyskland, Ungarn, Italien, Norge, Spanien og Sverige. Resultatet af borgertopmøderne vil blive overbragt til EU i juni 2014 og vil efterfølgende blive offentliggjort.

Dette informationshæfte indeholder den grundlæggende information om de problemstillinger, som blev diskuteret på det danske SurPRISE borgertopmøde i januar

2014. Det informerer også om de nye sikkerhedsteknologier, som SurPRISE undersøger. Endvidere indeholder det baggrundsinformation om overvågning, sikkerhed og privatliv i Europa.

Vi er klar over, at det kan være en udfordring at læse dette informationshæfte. Du behøver ikke at forstå hvert eneste ord, før du kommer til borgertopmødet. Vi har ikke tænkt os at teste dig i indholdet, og det er ikke vores hensigt at forsøge at gøre dig til ekspert på området. Formålet med denne bog er at give dig en idé om de emner, som vil blive diskuteret på borgertopmødet, og at få dig til at begynde at tænke over dine egne synspunkter om overvågning, privatliv og sikkerhed. Din deltagelse i borgertopmødet er vigtig, netop fordi du ikke er ekspert. Vi har bedt dig om at deltage, fordi du er en almindelig borger, hvis hverdagsliv påvirkes af de beslutninger, som europæiske og danske politikere træffer.

SurPRISE vil gøre beslutningstagerne og deres repræsentanter klogere på borgernes synspunkter. Sikkerhedsteknologier hænger sammen med menneskerettigheder, retfærdighed, civilsamfundets udvikling og pålidelige, effektive institutioner. Dette er årsagen til, at offentligheden bør involveres i disse anliggender – de angår ikke kun politikere og beslutningstagere, industrien, eksperter og ngo'er.

Politikerne bestemmer, hvordan sikkerhedspolitikken skal udformes, men som borger vil du komme til at leve med konsekvenserne af deres beslutninger. Derfor er din mening vigtig.

Videnskaben giver os information, men den fortæller os ikke, hvad vi skal gøre. Valget er dit. Giv din mening til kende!

1.1 Hvordan dette informationshæfte skal læses

Dette hæfte består af fem hovedafsnit. Det første er en generel introduktion til overvågning, sikkerhed og privatliv i Europa. De tre følgende afsnit skitserer de tre sikkerhedsteknologier, som vil blive diskuteret på borgertopmøderne. På det danske borgertopmøde vil vi dog kun diskutere avancerede overvågningskameraer og smartphone tracking. Hvert afsnit beskriver, hvorfor teknologien blev udviklet, hvordan den bliver brugt, hvilke forbedringer af sikkerheden den tilbyder, og hvilke begrænsninger den har. Desuden er der en faktaboks, som forklarer, hvordan teknologien virker. Det femte afsnit diskuterer kort nogle alternativer til sikkerhedsteknologierne.

Hvis du ikke vil læse hele hæftet, kan du nøjes med resuméet, der opsummerer hovedpointerne.

2 Resumé

SurPRISE forsøger at forstå de europæiske borgeres mangfoldige synspunkter på nye sikkerhedsteknologier. I takt med at europæiske regeringer er blevet mere optaget af terrorisme, organiseret kriminalitet og cyberkriminalitet, har de i stigende grad investeret i udviklingen af nye sikkerhedsteknologier.

Mange af disse teknologier analyserer information om borgeres adfærd i dagligdagen. Information fra for eksempel mobiltelefoner, internettet og 'intelligente' teknologier som digitale overvågningskameraer bruges til at identificere kriminelle og terrorister, nogle gange før de gør noget ulovligt.

Vi kalder disse teknologier for 'overvågningsorienterede sikkerhedsteknologier', fordi de benytter personlige oplysninger. En overvågningsorienteret sikkerhedsteknologi er:

en teknologi som benytter information om den brede befolkning indsamlet på forskellig vis for at håndtere et sikkerhedsproblem.

På SurPRISE borgertopmødet vil vi undersøge fem af disse teknologier til bunds:

- **Avancerede overvågningskameraer:** Overvågningssystemer, som rækker ud over simpel videoovervågning af det offentlige rum. De avancerede digitale kameraer er koblet sammen i et system, der kan identificere mennesker, analysere deres adfærd og spore bestemte genstande.
- **'Civile' droner:** Civile droner er ubemandede luftfartøjer (UAVs) til ikke militært brug. De kan bruges til en bred vifte af overvågningsaktiviteter. En drone kan udstyres med et kamera og andre sensorteknologier, og de kan betragtes som mobile versioner af overvågningskameraer.
- **Overvågning af internettet ved hjælp af 'deep packet inspection':** Beskeder og information, som sendes over internettet, kan læses, analyseres og ændres med særligt udstyr og programmer.

➤ **Smartphone tracking:**

Ved at analysere data, der viser hvor en mobiltelefon har befundet sig, kan der samles information om telefonbrugerens placering og bevægelsesmønster over en tidsperiode. En telefons placering kan bestemmes ud fra informationer fra de telefonmaster, den har været forbundet til, eller mere præcist gennem GPS eller forbindelser til trådløse netværk.

➤ **Biometri:**

biometri referer til automatiserede måder at genkende individer baseret på opmåling af deres fysiske eller adfærdsmæssige karakteristika. Den mest anvendte brug af biometri er det biometriske pas baseret på ansigts-, fingeraftryks- og/eller irisgenkendelse.

Hver af disse teknologier forbedrer sikkerheden ved at identificere mistænkelige personer samt kriminelle eller ulovlige aktiviteter. De kan også gøre livet meget lettere. Men hver sikkerhedsteknologi har alligevel sine ulemper. For eksempel fungerer avancerede overvågningskameraer eller civile droner udstyret med et kamera kun under bestemte forhold og kan i høj grad give anledning til 'falsk alarm.' 'Deep packet inspection' krænker privatlivets fred i online kommunikation. Smartphone tracking er svært at kontrollere, fordi mange applikationer sender placeringsdata fra telefonen uden brugerens vidende. Data der lækkes fra biometriske databaser kan muligvis resultere i identitetstyveri. Manglen på kontrol over indsamling og brug af information er et gennemgående problem med alle de teknologier, vi undersøger.

Brugen af disse teknologier rejser spørgsmål omkring menneskerettigheder, privatliv, regulering og tillid. Disse teknologier indsamler og deler sædvanligvis information om en person uden deres vidende. Data om uskyldige mennesker vil uundgåeligt blive indsamlet og analyseret, og for nogen teknologieres vedkommende, med fuldt overlæg. Derfor har de mulighed for at invadere privatlivet, som er en fundamental menneskeret i Europa. Uskyldige mennesker kan også risikere,

ved et uheld, at blive forvekslet med lovbrydere, med seriøse konsekvenser for deres liv til følge.

På trods af de forbedringer af sikkerheden, som teknologierne tilbyder, er nogle borgere usikre på, hvordan de egentlig vil have det med, at information om dem bruges til sikkerhedsformål. Hvis det gør alle mere sikre, er det måske i orden? Men hvis fundamentale menneskerettigheder bliver krænket, er det måske ikke i orden? Og måske afhænger folks mening også af, hvordan de ser på en række andre forhold, for eksempel:

- Virker teknologierne i det hele taget?
- Hvor krænkende er de?
- Kan man stole på de institutioner, der benytter dem?
- Er den juridiske kontrol effektiv og fyldestgørende?
- Hvem holder øje med dem, der overvåger?
- Hvad er der af alternativer?

Det er nogle af de spørgsmål, vi skal diskutere på borgertopmødet.

(Natur)videnskabsundervisning, forbrugeroplysning og især offentlige kontroverser om videnskab og teknologi er afgjort vigtige pointer for borgeres muligheder for at deltage i debatterne og udøve deres demokratiske rettigheder.

I de kommende afsnit, vil vi introducere nogle nøglebegreb og definitioner før vi beskriver fem udvalgte teknologier som bliver forklaret mere detaljeret.

Læs venligst videre for at lære mere om disse problematikker.

3 En helt almindelig dag...

Syd for Budapest svinger Aisha ind på motorvej E-75 mod den internationale lufthavn i Ferihegy. Hun tænker på den første gang, hun benyttede denne rute. Dengang betalte hun vejafgiften manuelt på stedet, nu bliver den automatisk trukket på hendes bankkonto. Hendes nummerplade bliver aflæst af ANPR kameraer, som er et automatisk nummerpladegenkendelsessystem, og vejafgiftssystemet ordner resten. Tidligere bemærkede Aisha ikke kameraerne højt oppe i luften. Nu ser hun dem og undrer sig over, hvordan den information, de opsamler, forbindes til hendes bank.

Aisha parkerer sin bil og stiger på shuttle-bussen, der kører hende hen til terminalen. Her tjekker hun ind på sit fly via en selvbetjeningsmaskine. Hun lægger sit pas på maskinen, som matcher hendes navn med detaljerne i hendes booking. Den printer herefter hendes boardingpas, og det går op for Aisha, at også den gemmer information om hende.

Da Aisha er gennem sikkerhedstjekket, smider hun sin håndbagage i en stol i kaffebaren og bestiller en kop kaffe. Hun tøver et øjeblik, før hun rækker sit kreditkort til ekspedienten. 'Det er godt nok smart med det plastickort,' tænker hun, 'men hvem er det egentlig, der registrerer denne transaktion?'

Mens Aisha venter på sin kaffe, tager hun sin smartphone frem for at tjekke, om hun har fået nogen beskeder. Skærmen lyser op, og telefonens placeringsdata ændres øjeblikkeligt fra 'Kecskemét,' hvor Aisha bor, til 'Ferihegy.' 'Hvordan kunne den vide det? Der må være en logisk og indlysende forklaring, men jeg kan bare ikke lige regne det ud,' funderer hun.

Aisha kan lige nå at sende en e-mail til en arbejdskollega, inden hun skal stige om bord på flyet. Hun sætter telefonen på flight mode og spekulerer på, hvad der mon sker med e-mailen på dens vej gennem internettet.

Aishas oplevelse er ikke usædvanlig. De begivenheder, den består af, kender enhver rejsende. Teknologierne gør Aishas rejse mere bekvem og effektiv, men de giver også anledning til spørgsmål: Hvem bruger mine personlige data, og hvad betyder det for mig, at de er registreret i 'systemet'?

Mange af de teknologier, Aisha støder på, findes også uden for lufthavnens verden. Masser af mennesker kunne slet ikke forestille sig et liv uden smartphone, kreditkort og internet! I virkeligheden er der masser af hverdagsaktiviteter, der er forbundet med den form for elektronisk dataregistrering, som Aisha er blevet opmærksom på. Måske stiller du også dig selv sådanne spørgsmål indimellem. Dataregistrering kan angive vores placering i tid og rum, og somme tider endda også fortælle, hvad vi foretager os. For eksempel kan banktransaktioner vise, hvad vi køber, og hvem vi handler med. Disse data

findes i bankens databaser, og vi kan se dem på vores kontoudtog.

Flyselskaberne er i besiddelse af vores billetreservationer, som kan vise, hvorvidt vi rejser til eller fra en risikobetonet del af verden. Data fra vores mobiltelefoner kan angive vores placering, hvem vi taler med, og hvor ofte vi gør det. Den europæiske lovgivning sikrer, at telefonselskaberne og internetudbydere gemmer informationen i deres faktureringsdatabaser. Derfor er det muligt at identificere, lokalisere og spore de fleste mennesker på forskellige tidspunkter i deres liv. Det er måske det, der bekymrer Aisha, men hun har alligevel blandede følelser omkring det, da teknologierne jo også rummer mange fordele.

Sådanne teknologier og den information, de indsamler, kan også gavne andre. For at kunne følge og opklare terrorangreb i og uden for

Europa har politikerne investeret i avancerede sikkerhedsteknologier, som betjener sig af denne form for information. De har også ændret eksisterende lovgivning og udstedt nye love for at tillade adgang til informationen til sikkerhedsformål. Selvom der findes mange 'officielle' efterretningskilder, har man indset, at potentielle kriminelle og terroristers aktiviteter måske også kan spores på andre måder. Ligesom alle andre har kriminelle og terrorister bankkonti og personlige identifikationspapirer, og de bruger også internet og mobiltelefon. De benytter forskellige former for transport, opholder sig i det offentlige rum og forbruger varer og serviceydelser. Måske kan mere viden om disse aktiviteter være nøglen til at finde kriminelle og terrorister. Mange myndigheder mener, at man ved hjælp af nye sikkerhedsteknologier ikke blot vil være i stand til at finde og arrestere synderne, men også vil kunne identificere dem, før de begår en kriminel handling. Fordi teknologierne bruger information på denne måde, kalder SurPRISE projektet dem for 'overvågnings-orienterede sikkerhedsteknologier.'

En overvågnings-orienteret sikkerhedsteknologi er:

en teknologi, der benytter information om den brede befolkning indsamlet på forskellig vis til at håndtere et sikkerhedsproblem.

Hvis Aisha tænkte på, at informationen om hende kunne bruges på denne måde, ville hun så fortsat nære blandede følelser? Hvis det betød bedre sikkerhed for hende og alle andre, ville hun måske have nemmere ved at acceptere det. Brugen af disse teknologier rejser imidlertid spørgsmål om menneskerettigheder, privatliv, kontrol og tillid. Teknologierne indsamler og videregiver undertiden information om mennesker uden deres vidende. Uskyldige menneskers data bliver uundgåeligt indsamlet og analyseret, og når det gælder visse af teknologierne, sker det med fuldt overlæg. Teknologierne har således potentiale til at true privatlivets fred, som i Europa er en grundlæggende menneskerettighed. De kan også medføre, at uskyldige mennesker bliver mistænkt

for kriminalitet, med alvorlige konsekvenser til følge.

Det rejser også en række andre spørgsmål:

- Er de institutioner, som bruger disse data, til at stole på?
- Hvor meget kontrol er der med de institutioner, som bruger disse data?
- Bliver teknologierne brugt i overensstemmelse med loven?
- Er institutionerne til at få indblik i, og bliver de holdt ansvarlige for eventuelle krænkelse af privatlivets fred foretaget i sikkerhedens navn?
- Forbedrer disse teknologier virkelig sikkerheden?

Dette er nogle af de spørgsmål, som vi vil tage op på borgertopmødet.

I de næste afsnit introduceres nogle nøgleord og definitioner, hvorefter vi vil beskrive de tre teknologier, som vi skal fordybe os i på borgertopmødet.

3.1 Overvågning, privatliv og sikkerhed

3.1.1 Overvågning

Når vi tænker på 'overvågning', er der sandsynligvis et par billeder, der straks dukker op på nethinden: Du tænker måske på 'Big Brother' – både reality tv-serien og karakteren i George Orwells roman 1984. Derfor forbinder du måske overvågning med en ubehagelig fornemmelse af at blive holdt øje med af en magtfuld, men ukendt person eller organisation.

Når vi i SurPRISE taler om 'overvågning', tænker vi på det som et spørgsmål om 'at holde øje med mennesker for at kunne kontrollere eller styre deres adfærd.' Dette kan gøres af forskellige årsager og tjene forskellige formål. Overvågning kan

foretages af sikkerhedshensyn. Politiet kan benytte overvågningskameraer eller droner udstyret med overvågningskameraer for at kunne identificere lovovertrædere i gadebilledet. Overvågning kan også tjene kommercielle formål. For eksempel kan en butik betjene sig medlemskort for at registrere, hvilke varer forskellige kundegrupper foretrækker at købe. Dette kan igen bruges til at fastlægge, hvilke særlige tilbud kunderne skal have i fremtiden. Overvågning kan bruges til at forebygge kriminalitet og fange kriminelle, men det bruges også til at forsyne mennesker med varer og serviceydelser.

Hvis overvågning er en fast del af samfundet, undrer du dig måske over, hvad der så er i vejen med det. Nyheder, som har at gøre med 'overvågningssamfundet', synes altid at have et ildevarslende skær over sig. Pointen er, at det giver stor magt at råde over en overvågningsteknologi. Det er vigtigt at dem, der har mulighed for at udnytte denne magt, det være sig politimyndigheder eller forretningsforetagender, bruger deres magt på en måde, der er lovlig, retfærdig og i overensstemmelse med borgernes rettigheder.

Måske synes du ikke selv, at du har noget at skjule eller frygte, men det vil afhænge af, hvem der overvåger dig, hvorfor de overvåger dig, og hvordan de opfatter dine handlinger. Hvis du ikke har nogen kontrol med processen, ikke har mulighed for at gøre indsigelser, og reglerne pludselig bliver ændret i strid med dine interesser – måske på grund af din etnicitet, religion, seksuelle orientering, køn eller politiske synspunkter – hvad vil du så gøre? Dette er årsagen til, at overdreven brug af overvågning kan have en negativ indflydelse på andre menneskerettigheder såsom ytringsfriheden. Under disse omstændigheder kan overvågning også skade den sociale tillid i samfundet, idet folk måske begynder at frygte at være sig selv. Meget er uvist, når forskellige former for overvågningsdata bliver brugt i en sikkerhedskontekst.

3.1.2 Privatliv og databeskyttelse: vigtige spørgsmål

Blandt de helt store spørgsmål er hensynet til privatlivets fred og beskyttelsen af de data, som de nye sikkerhedsteknologier skaber og gør brug af. Selvom privatlivet kan betyde forskellige ting for forskellige

mennesker, er det en vigtig del af det at være menneske til daglig. Der er en række ting, som du måske nok har lyst til at holde for dig selv på forskellige tidspunkter:

- hvad du laver, tænker og føler
- information om dine intime relationer, hvor du er, hvad du fortæller andre, dine særlige kendetegn og dit selvbillede
- din krop: hvor meget af den, du har lyst til at vise frem, hvorvidt du kan undgå uønskede berøringer eller kropsvisiteringer, og din kontrol over andres adgang til dit kropslige materiale, såsom din dna og dit fingeraftryk.

Prøv at tænke over, om du ville være tilfreds med, at det forsikringsselskab, hvor du har din livsforsikring, havde ubegrænset adgang til din lægejournal. Eller hvis politiet kunne lytte til alle dine telefonsamtaler. Har du gardiner i dit hjem? Hvis du svarer 'nej' til de to første spørgsmål og 'ja' til det tredje, bekymrer du dig sandsynligvis alligevel om dit privatliv. Det er du ikke ene om. Studier af unge mennesker, der bruger sociale medier, viser, at de af frygt for krænkelser af privatlivets fred er meget selektive med, hvilken information de offentliggør om sig selv. Folk har fortsat lyst til at dele information, men de ønsker at gøre det inden for en etableret ramme, og det er denne ramme, der markerer, hvor privatlivet begynder.

I SurPRISE definerer vi privatliv som:

et individs mulighed for at være i fred, ude af offentlighedens søgelys og selv herre over information om sig selv.

Retten til privatliv er en grundlæggende menneskerettighed i Europa. Alle har brug for denne ret: til at være frie til at handle, mødes og diskutere i et demokratisk samfund. Demokratisk frihed kan slet ikke udøves, hvis folks tanker, intentioner og

handlinger er kendt på forhånd. Ny europæisk databeskyttelseslovgivning vil kræve, at hensynet til privatlivets ukrænkelighed bliver indskrevet i selve designet af nye teknologier, så disse allerede i udgangspunktet vil være mindre krænkende i forhold til privatlivets fred. De virksomheder, der laver nye teknologier, vil blive opfordret til at forholde sig til privatlivets ukrænkelighed på alle niveauer i processen. Denne nye tilgang kaldes 'privacy by design' – design-baseret sikring af privatlivets fred.

- at øge sikkerheden på internettet for borgere og virksomheder i EU
- at infiltrere internationale kriminelle netværk
- at afværge terrorisme
- at øge EU's evne til at komme på fode igen efter forskellige former for kriser og ulykker

3.1.3 Sikkerhed

I SurPRISE projektet definerer vi sikkerhed som:

en tilstand af at være beskyttet mod eller ikke udsat for fare – en følelse af tryghed og fravær af eller afskærmethed mod fare.

Sikkerhed har ikke kun at gøre med beskyttelse af fysiske genstande såsom bygninger, informationssystemer, landegrænser osv., det har også at gøre med den menneskelige følelse af sikkerhed. I en ideel verden ville effektive sikkerhedsforanstaltninger resultere i en øget følelse af sikkerhed, men i virkeligheden er det ikke altid tilfældet.

Det virker paradoksalt, at de nye sikkerhedsteknologier i kraft af deres potentiale til at true privatlivets fred i sidste ende kan få os til at føle os mindre sikre – i stedet for at øge vores følelse af sikkerhed. Men situationen er sandsynligvis ikke ens for alle. Ligesom det er tilfældet med privatlivet, betyder sikkerhed noget meget forskelligt for forskellige mennesker. Vi har alle vores egne opfattelser af, hvad vi betragter som en trussel mod sikkerheden, og hvor langt vi vil gå for at beskytte det, der er vigtigt for os.

Dette gælder også for dem, der bestemmer, hvordan sikkerheden skal forvaltes. De bliver nødt til at identificere og forholde sig til de vigtigste trusler. Myndighederne vil have begrænsede økonomiske, menneskelige og tekniske ressourcer til sikkerhedsformål, og derfor er det nødvendigt at træffe nogle valg. For EU er hovedprioriteterne med hensyn til sikkerhed:

Eftersom EU har bestemt sig for at fokusere på genrejsning efter kriser og ulykker, rækker sikkerhed nu langt ud over afværgelse af kriminalitet og terrorisme. EU bekymrer sig også om trusler mod miljøet, naturressourcer, infrastrukturer, økonomiske aktiviteter og sundheden. For de politiske beslutningstagere har sikkerhedsaspektet bredt sig ind i næsten alle sfærer af det offentlige liv. Denne tilgang har mange lande i EU tilsluttet sig. Men kan dette løfte om sikkerhed på alle disse områder nogensinde indfries? Blandt andet for at kunne dække dette behov er sikkerhedsindustrien i disse år ved at udvikle sig til en hovedindustri i Europa. Den indbefatter store selskaber som Airbus, BEA Systems og Finmeccanica samt en lang række mindre selskaber. De seneste udviklinger inden for overvågningsorienterede sikkerhedsteknologier indbefatter:

- Avancerede overvågningskameraer med fokus på at genkende lovovertrædere og identificere mistænkelig adfærd, før en forbrydelse er begået
- Overvågning af internettet for at afværge skader forårsaget af virus, hackere eller identitetstyveri
- Biometri, som bruges til at forhindre uønskede individer i at få adgang til et givet område og til at fremskynde adgangsproceduren for de mennesker, som myndighederne kender som 'lovlige rejsende'

- Droner, som kan registrere adfærd fra luften, der ikke kan ses fra jorden. Denne information kan bruges til at dirigere sikkerhedspersonel hen til steder, hvor der er ved at opstå problemer
- Avancerede passagerdata-systemer, der søger at identificere individer, som kan udgøre en trussel
- Placeringsmæssige sporingsteknologier, der søger at reducere skader på ting i bevægelse og at udpege mistænkelige personer i det offentlige rum

4 Fem nye sikkerhedsteknologier

De fem sikkerhedsteknologier, der bliver undersøgt i SurPRISE-projektet er:

- **Avancerede overvågningskameraer**
- **Droner**
- **Overvågning af internettet ved hjælp af 'deep packet inspection'**
- **Smartphone tracking**
- **Biometri**

Disse sikkerhedsteknologier er fortsat under udvikling, og lovgivningen omkring dem er ikke fastlagt endnu.

de følgende afsnit i informationshæftet bliver der redegjort for, hvordan hver af de tre teknologier fungerer, hvorfor den enkelte teknologi blev udviklet, og hvordan den bruges i dag. Der vil også blive redegjort for, hvilke sikkerhedsforbedringer den enkelte teknologi tilbyder, og hvordan privatlivets fred og andre forhold påvirkes af den.

Det er vigtigt for dette projekt – og for EU – at finde ud af, hvad borgerne synes om sikkerhedsteknologier, og i hvor høj grad de kan acceptere dem. Det er derfor, din mening er så vigtig. Måske er du allerede tilhænger eller modstander af nogle af teknologierne. Under SurPRISE borgertopmødet vil du få rig mulighed for at ytre din mening, men vi vil i særdeleshed gerne have dig til at tænke over følgende spørgsmål

Hvilke af disse faktorer er afgørende for, om du kan acceptere en sikkerhedsteknologi?

Kunne det for eksempel være:

- > Mere viden om teknologien og hvordan den virker?
- > Mere viden om, hvordan forskellige institutioner bruger teknologien og den information, den producerer?
- > Effektiv juridisk rådgivning og kontrol?
- > Bedre information om de trusler, vi står overfor, og som teknologien er skabt til at bekæmpe?

Eller handler det om, hvor krænkende du mener teknologien er? For eksempel:

- > Sætter den folk i forlegenhed?
- > Krænker den dine rettigheder som borger?
- > Videregiver den information til tredjeparter uden dit vidende, eller har den indflydelse på andre områder af dit privatliv?

Måske handler det om, hvor effektiv teknologien er:

- > Gør den dit liv mere bekvemt?
- > Får den dig til at føle dig mere tryk?
- > Er den efter din mening et præcist værktøj til at identificere mistænkte med?

Måske tænker du kun over tilstedeværelsen af sikkerhedsteknologier, når du er opmærksom på dem i dine umiddelbare omgivelser. Det kunne være i lufthavnen, når du går på gaden, eller når du bruger din mobiltelefon eller går på nettet. Resten af tiden generer de dig ikke. Måske har du det fint med sikkerhedsteknologier i dag, men bekymrer dig om, hvordan de vil blive brugt i fremtiden

5 Avancerede overvågningskameraer

Tidligere i dette informationshæfte beskrev vi, hvordan Aisha undrede sig over, hvordan kameraerne sørgede for, at vejafgiften blev hævet på hendes bankkonto. Kameraerne var ANPR kameraer, der benytter automatisk nummerpladenkendelse. ANPR kameraer er et eksempel på en ny sikkerhedsteknologi, der kaldes 'avancerede overvågningskameraer.'

De fleste europæere kender til overvågningskameraer. Et 'traditionelt' kameraovervågningssystem består af kameraer, som er hængt op i butikker eller i det offentlige rum. Kameraerne er forbundet til et kontrolrum via telekommunikation. I kontrolrummet kan operatører på et antal skærme studere de billeder, som kameraerne indfanger. Billederne bliver optaget, gemt og slettet igen efter et stykke tid. Systemet er 'lukket', idet billederne ikke bliver fremvist andre steder end i kontrolrummet. Hvis operatørerne ser noget mistænkeligt, kan de kontakte sikkerhedsvagterne eller politiet, så disse kan tage affære.



5.1 Baggrunden for udvikling af overvågningskameraer

Overvågningskameraet blev oprindelig udviklet til overvågning af raketopsendelser under 2. verdenskrig og for at kunne håndtere risikable eller sundhedsfarlige industriprocesser på afstand. Det blev først markedsført som en sikkerhedsteknologi i USA i 1950'erne og efterfølgende indført af politiet i USA og i England i 1960'erne. Brugen af overvågningskameraer voksede støt overalt i Europa i 1990'erne, anført af England og skarpt forfulgt af Frankrig og Holland. Og teknologien optræder meget ofte i nyhedsmedierne. Overvågningskameraer var for eksempel altafgørende i forbindelse med identificeringen af de ansvarlige bag bombeangrebet mod Boston Marathon i 2013.

Avancerede overvågningskameraer er designet til at løse de problemer, som overvågningskameraet har kæmpet med siden begyndelsen. Blandt andet at der er alt for mange kameraer og alt for få sæt øjne til at holde styr på, hvad der foregår. I modsætning til et 'traditionelt' overvågningssystem benytter et avanceret overvågningssystem sig af netværksforbundne digitalkameraer, som er forbundet til systemer, der kan analysere de digitale billeder. Software analyserer, hvad der foregår på billedet. Hvis noget usædvanligt er på færde, aktiverer det en alarm, der tilkalder en operatør. Disse alarmer bliver i sig selv registreret og systematiseret, således at de billeder, der forbindes med alarmen, gemmes på en computer og nemt kan genfindes og deles.

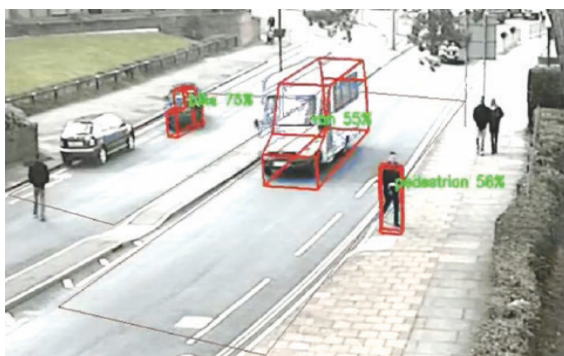
Når kameraerne kobles sammen med avancerede computerprogrammer, kan de bruges til mange forskellige formål. De bliver som oftest brugt til:

- at identificere genstande på et billede, såsom et køretøj, ved at aflæse nummerpladen og sammenligne den med information i en database
- at identificere en persons ansigt, når dette vises på en neutral baggrund. For at

identificere personen sammenlignes dette billede med billeder af personer registreret i en database

- at identificere en efterladt taske i det offentlige rum

Selvom avanceret kameraovervågning endnu ikke er en fuldstændig pålidelig teknologi, er der computerprogrammer under udvikling, som kan gøre følgende:



- identificere personer i en folkemængde ved at spore deres påklædning
- identificere mistænkelig adfærd eller adfærd, der forekommer usædvanlig i forhold til omgivelserne. Adfærden på billederne sammenlignes med kendte adfærdsmønstre, som er lagret i en database.

Kameraovervågningssystemerne er imidlertid ikke ens. Hvor 'avanceret' et kameraovervågningssystem er, afhænger af, hvor godt computerne analyserer et billede, og hvad der sker med dette billede, efter at det er blevet registreret. Systemer installeres af forskellige årsager, så det er ikke sikkert, at et givet intelligent overvågningssystem kan alle de ting, der er nævnt her. Måske har ejeren af systemet ikke brug for alle disse funktioner.

Sådan virker avancerede overvågningskameraer

Ved at bruge 'intelligente algoritmer' lærer en computer, som er forbundet til et intelligent overvågningssystem, at genkende særlige typer af offentlig adfærd. Disse adfærdstyper kaldes 'trigger events.' Det kan for eksempel være en person, der står med et skydevåben eller en person, der står stille i en folkemængde i bevægelse. En algoritme er en række udregninger, der filtrerer de dataoplysninger, som det digitale billede indeholder. En intelligent algoritme lærer, hvad den leder efter, i takt med at den analyserer mere og mere data.

Algoritmer i intelligente overvågningssystemer er designet til at kopiere, hvordan det menneskelige øje og den menneskelige hjerne fungerer. Softwaren nedbryder et billede i små bitte dele, der kaldes 'pixels.' Du kender sikkert begrebet 'pixel', hvis du har et digitalt kamera eller en smartphone.

Hvis et digitalt kamera har '3 megapixels', består hvert billede af 3 millioner pixels.

Algoritmen er i så fald i stand til at udregne graden af bevægelse for hver pixel i et billede. Dette sætter computerprogrammet i stand til at identificere de aktive områder i hvert optrin. På denne måde lærer det at genkende bevægelsesmønstrene i en given situation. På denne måde kan systemet identificere og klassificere begivenheder i forhold til mønstre, det allerede kender. For eksempel kan computerprogrammet skelne mellem passive tilskuere og fans, der hopper op og ned under en fodboldkamp.

5.2 Brugen af avancerede overvågningskameraer

Avancerede kameraovervågningssystemer er kommercielle produkter, der forhandles af sikkerhedsfirmaer og våbenleverandører. Adskillige systemer er allerede i handlen. De primære institutioner, som i dag benytter sig af avanceret kameraovervågning, er transportmyndigheder, såsom motorvejs-, lufthavns-, havne- og jernbanemyndigheder samt de kommunale myndigheder og politiet.

I Budapest begyndte politiet i slutningen af 2012 at anvende avancerede overvågningsskameraer til at observere busruter. Politiet kan lovligt anvende disse overvågningsbilleder, så længe passagererne ikke filmes, og så længe offentligheden er informeret om overvågningen. Ansigtsgenkendende kameraer har været brugt i Zürich lufthavn siden 2003. På det tidspunkt var dette den første brug af ansigtsgenkendelse nogensinde i forbindelse med grænsekontrol. Dette system er nu permanent installeret.

EU har finansieret 16 forskellige projekter, der skal udvikle algoritmer og funktioner til avancerede kameraovervågningssystemer. I dag er de mere komplekse anvendelsesmuligheder, såsom genkendelse af mistænkelig adfærd eller ansigter i folkemængder, under fortsat udvikling og forbedring. Denne brug er dog ikke særlig udbredt, men der bliver hele tiden testet nye systemer. For eksempel har transportmyndighederne i Rom, London, Paris, Bruxelles, Milano og Prag for nylig deltaget i afprøvnin-gen af et



fodgænger-overvågningssystem, der betjener sig af avanceret kameraovervågning.

Dette system henleder operatørernes opmærksomhed på mistænkelige genstande samt unormale bevægelser og usædvanlig adfærd blandt passagererne. Systemet er endnu ikke taget i anvendelse og er fortsat under afprøvning på nuværende tidspunkt.

Den mest udbredte anvendelse af avanceret kameraovervågning er sandsynligvis automatisk nummerpladegenkendelse. Med et digitalt billede af en bils nummerplade kan informationerne sammenholdes med statslige databaser over bilejere, databaser fra forsikringsselskaber og politiets databaser. Bilens ejer og dennes folkeregisteradresse kan nemt identificeres, og ANPR kameraet kan nøjagtigt angive et bestemt individs placering i tid og rum. Dette system kan bruges til at identificere stjalne køretøjer, køretøjer uden forsikring, køretøjer benyttet uden betaling af afgifter eller køretøjer, der ikke overholder fartgrænserne.

Spørgsmålet er, om de forskellige lovovertrædelser alle retfærdiggør samme grad af overvågning. Bør avancerede overvågningsskameraer benyttes til at forebygge alle slags lovovertrædelser eller udelukkende til de farligste af dem? Der er forskellige holdninger til avanceret kameraovervågning i Europa. I Tyskland indskrænkede forfatningsdomstolen

Kontrovers i forbindelse med intelligent overvågning: ANPR i Birmingham

I 2011 blev politiet i Birmingham, England, nødt til at fjerne ANPR kameraer fra tre områder i byen, der havde en høj koncentration af muslimske borgere. Kameraerne var finansieret af et anti-terror program ved navn 'Project Champion,' men over for offentligheden blev opsættelsen af kameraerne begrundet med, at de tjente et sikkerhedsmæssigt formål i forhold til at forhindre overfald, tyverier mm. Lokalrådsformænd såvel som lokale politikere protesterede i stærke vendinger mod opsættelsen af kameraerne, og relationerne i lokalsamfundet blev skadet. 200 kameraer blev installeret men aldrig tændt. 64 af kameraerne var skjulte og blev sat op uden offentlighedens vidende. Kameraerne blev enten ødelagt eller brugt af andre politistyrker i England. Det fejlslagne projekt og tabet af kameraerne kom til at koste politiet 300.000 pund.

i 2008 for eksempel politiets brug af ANPR med henvisning til privatlivets fred. Domstolen fastholdt, at politiet kun var berettiget til at opbevare digitale data indsamlet ved hjælp af ANPR kameraer, hvis der øjeblikkeligt blev foretaget database-tjek og udført de nødvendige sanktioner. ANPR bruges endvidere til at opkræve vejafgifter i Tyskland, men dette bliver ofte kritiseret, eftersom der også findes andre og mindre overvågningsbaserede metoder til at opkræve disse afgifter. I London bruges ANPR ligeledes til at opkræve vejafgifter, og til forskel fra i Tyskland er systemet nu en integreret del af både lokale og nationale politistategier i England. Siden 2010 er der blevet installeret 5.000 ANPR kameraer i England, hvor det nationale politis datacentral behandler mellem 10 og 14 millioner ANPR optagelser hver eneste dag.

5.3 Sikkerhedsforbedringer

Avanceret kameraovervågning kan forbedre sikkerheden på følgende måder:

1. Sikkerhedsproblemer bliver nemmere at opdage samtidig med at de indtræffer:
 - Systemet identificerer enhver usædvanlig hændelse og henleder operatørens opmærksomhed herpå via en alarm. Dette gør det nemmere for operatøren at fortolke billederne.
 - Alarmen gør det nemmere for operatøren at træffe hurtigere, mere effektive beslutninger om, hvorvidt der skal gøres noget for at løse et sikkerhedsproblem.
 - Systemets algoritmer kan undertiden indfange detaljer, som en menneskelig operatør

kunne overse. Dette skyldes, at de kan håndtere meget store mængder information.

2. Angsten for kriminalitet reduceres:
 - Når sikkerhedsteknologien fungerer effektivt, føler folk sig trygge, fordi de ved, at enhver usædvanlig hændelse, der finder sted omkring dem, hurtigt vil blive opdaget af et intelligent overvågningssystem.
 - Avancerede overvågningskameraer kan registrere langt flere detaljer end traditionelle overvågningskameraer. Dette betyder, at der er brug for færre kameraer til at overvåge et område. Som resultat heraf kan intelligent overvågning føles mindre krænkende, fordi der ikke er så mange kameraer.
 - Der kan værnes mere om privatlivets fred, fordi følsomme områder såsom privat grunde kan 'mørklægges' på billederne, så operatøren ikke ser dem.

5.4 Problemer

Der er dog adskillige ulemper ved avanceret kameraovervågning, som man er nødt til at holde sig for øje:

1. De intelligente overvågningsalgoritmer, som anvendes i dag, har mange skavanker. Disse skavanker kan udløse en 'falsk alarm,' som fejlagtigt identificerer et sikkerhedsmæssigt optrin. Dette kan betyde, at en uskyldig person forveksles med en mistænkt. De aktuelle skavanker består i:
 - Kun specifikke objekter, såsom en bilnummerplade eller en efterladt taske på en tom plads, kan identificeres pålideligt.
 - Kameraerne er mindre gode til at identificere, hvad der foregår i en folkemængde.

- Skjulte forbrydelser, såsom lommetyveri eller butikstyveri, er svære at identificere.
 - Algoritmerne er sårbare over for fordomme, fordi de er programmeret af mennesker til at identificere, hvad disse betragter som usædvanligt. Der er en risiko for at systemerne – med fuldt overlæg eller ved en fejl – bliver programmeret til fokusere på minoriteter på en diskriminerende måde.
 - Hvis folk er opmærksomme på, at der bliver anvendt avanceret kameraovervågning, kan de undgå at blive sporet ved simpelthen at skifte tøj, eftersom algoritmerne fungerer ved at genkende det tøj, de mistænkte har på.
 - Det store antal falske alarmer, som de menneskelige operatører modtager, kan resultere i, at de taber tilliden til systemet og begynder at ignorere, hvad det fortæller dem.
2. Avancerede overvågningskameraer er både kraftigere og mindre:
- De kan indfange mere information og gør dermed potentielt et større indgreb i privatlivet, fordi uskyldige menneskers aktiviteter er mere udsat for at blive indfanget og analyseret.
 - Kameraerne er sværere at få øje på, hvilket gør det sværere for folk at vide, at de bliver overvåget. Derfor er det også sværere for folk at udfordre eller undgå overvågningen.
 - Hvis befolkningen opdager, at deres adfærd i det offentlige rum bliver overvåget af den nævnte kombination af computerprogrammer og operatører, kan det påvirke ytringsfriheden.
3. Der er stadig brug for mennesker til at håndtere systemerne:
- Der er behov for en person til at fortolke billederne og bekræfte, at der er tale om en berettiget alarm. Systemet kan identificere usædvanlig adfærd, men det kan ikke forklare, hvorfor denne adfærd finder sted.
 - Institutionerne bliver nødt til at være meget påpasselige med, hvem de rekrutterer til at arbejde med systemerne og oplære disse personer grundigt. De må være i stand til nøje at afpasse, hvilke former for undersøgelser der foretages, og sikre sig mod datamisbrug

’Der må være fuld gennemsigtighed med hensyn til, hvorfor vi benytter avanceret kameraovervågning. Folk har ret til at kontakte systemets driftsleder og spørge, hvordan det bliver brugt. De må vide, at der er en god grund til, at kameraet er der, og de må føle sig trygge ved, hvordan det bliver brugt.’

Chris Tomlinson, Independent Security Consultant



6. Droner

En drone er det flyvende element i et ubemandet luftfartøjssystem (UAS). Det flyves af en pilot via et kontrolsystem på jorden, eller autonomt ved hjælp af en computer ombord. Droner kaldes også Remotely Piloted Aircraft (RPA), Remotely Piloted Vehicle (RPV), eller Unmanned Aerial Vehicle (UAV). Brugen af droner har nydt øget offentlig opmærksomhed efter USA i højere grad begyndte at bruge droner i sin krig mod terrorisme i Afghanistan, Pakistan, Yemen og Somalia efter angrebene den 11. september. For nylig er også mange europæiske stater begyndt at udstyre deres militære styrker med droner.

Droner bruges ikke kun af militæret i krigslignende kontekst, men også myndighedsudøvere til rekognoscering og overvågning for at sikre civiles sikkerhed. Disse ikke militære 'civile' droner bliver i højere og højere grad brugt som flyvende kameraer der overvåger offentlige rum for at forhindre og opdage en bred vifte af sikkerhedstrusler. Civile droner bliver også brugt til ikke-sikkerhedsrelaterede opgaver, som for eksempel kartografi, ejendomsmægler fotos eller som legetøj. Et andet vigtigt aspekt er at de muliggør overvågning af områder der er for farlige for mennesker at bevæge sig i, for eksempel efter laviner, jordskælv, eller nukleare uheld. Eksempelvis blev droner brugt efter Fukushima ulykken til at overvåge værket tilstand og kontrollere strålningsniveauet.

SurPRISE projektet undersøger mulighederne med eksisterende og kommende overvågningsteknologier som midler til at skabe sikkerhed, derfor fokuseres der her primært på civile droner der bruges i sikkerhedsøjemed.



6.1 Hvorfor blev droner udviklet

Droner blev oprindeligt designet til militær rekognoscering og målrettede angreb med våben. Teknologien til at fjernstyre et ubemandet luftfartøj blev første gang brugt under Første Verdenskrig. Det første fartøj blev udviklet af Professor A. M. Low i Storbritannien i 1916. Det var designet til både forsvar mod de zeppelinere der blev styret fra jorden og som en flyvende bombe til hvilken det blev overvejet at lade den styre fra et bemannet fly der fulgte den.

Selvom droner i dag oftest bliver associeret med militær brug, bliver de i stadig højere grad brugt af civile offentlige myndigheder, virksomheder og private.

I EU bliver 'lette' droner der vejer under 150kg og alle droner brugt til sikkerheds- og militære formål reguleret af medlemsstaterne. Reguleringen af brugen af større droner til kommercielle formål bliver i øjeblikket undersøgt af Europa Kommissionen, som satser på begynde integrationen i EUs civile luftrum i 2016. I 2028 burde droner være fuldt integreret i EUs civile luftrum.

Igangværende forskning søger at gøre fremtidige droner endnu mindre afhængige af menneskeligt opsyn, og dermed at krydse grænsen til robotvidenskaben. Droner bliver udstyret med sensorer der muliggør at de kan flyve autonomt i byrummet. Nye metoder til masseproduktion af mini droner er også under udvikling. De teknologiske muligheder indenfor droneområdet er i hastig udvikling, eftersom prisen for at bygge og anvende droner fortsat falder.

Droner kan leveres med et stort udbud af forskellige udstyrmæssige tilføjelsesmuligheder, der muliggør overvågning og indgriben. Hvilken type tilføjelse der er mulig afhænger af størrelsen og bæreevnen for det enkelte fartøj.

6.2 Hvordan droner bliver brugt

Droner kan på effektiv vis bruges til at komplementere eksisterende infrastruktur (bemandet luftfartøjer eller satellitter) der bruges af offentlige aktører til at bistå krisehåndtering, myndighedsudøvelse, grænsekontrol, trafikovervågning og brandslukningsarbejde.

I en sikkerhedskontekst, har myndighedsudøvere i EU primært brugt droner til at overvåge

menneskemasser ved store offentlige begivenheder så som musik festivaler, demonstrationer eller sportsbegivenheder, til at opfange usædvanlig begivenheder eller pludselige bevægelser i menneskemængder. De kan også bruges til gerningsstedsundersøgelser. Deres brug til grænsekontrol er også en mulighed der vil blive udnyttet mere i EU i den nærmeste fremtid. Droner har også været brugt til at opfange dyrkning af forbudte stoffer og som support i politijagter.

Overvågningsdroner brugt til at overvåge offentlige rum har en stor forholdsmæssig fordel. De kan overvåge et meget større område, de er mobile og brugen af dem i 50 til 200 meter tillader et andet perspektiv sammenlignet med de mere statiske offentlige overvågningskameraer.

Droner kan bruges til en lang række kommercielle formål. De kan bruges som en del af præcisionslandbrug og fiskerier, el og gasledningsovervågning, kommunikation og broadcast services, trådløs kommunikationsrelæ og satellitforstærkende system, overvågning af naturrigdomme, medie og underholdning, digital kortlægning, jord og vildt administration, eller luftkvalitetsadministrering og kontrol.

På trods af disse imponerende perspektiver, er der stadigvæk forskellige tekniske problemer der endnu ikke er løst. Disse omfatter for eksempel begrænsninger i forhold til flyvehøjde, fart og varighed, så vel som spørgsmål i forhold til genoptankning af droner under flyvning. Droner er også meget sårbare over for u hensigtsmæssigt vejr, så som tykke skyer, vind og regn. Derudover, skaber droner der genererer data via avanceret udstyr, så som overvågnings kameraer og sensorer, store arbejdsbyrder og udløser problemer med manglende båndbredde. Desuden kan overvågningsbilleder være utydelige på grund af dronens bevægelser.

7. Overvågning af internettet ved hjælp af 'deep packet inspection'

Mens hun sad i lufthavnens kaffebar, undrede Aisha sig over, hvad der egentlig skete med den e-mail, som hun sendte til sin kollega, mens den bevægede sig gennem internettet. Den kan meget vel være stødt på en internetovervågningsteknologi, som kaldes 'deep packet inspection.'

Internetudbydere, netværksoperatører og telefonselskaber har altid været i stand til at overvåge deres netværk. Viden om, hvem der kommunikerer med hvem, hvilke hjemmesider der besøges, og hvilke services der benyttes, anvendes til fakturering netværksstyring og marketing. Der findes imidlertid også en teknologi ved navn 'deep packet inspection' (herefter DPI), som sætter selskaber, efterretningstjenester og regeringer i stand til at læse indholdet af den kommunikation, der sendes via internettet. Man kan sige det på den måde, at DPI svarer til, at postkontoret åbner alle breve, læser dem, og nogle gange vælger at ændre i dem, slette dem eller ikke at levere dem. DPI er i stand til at overvåge alle aspekter af digital kommunikation. Fra den information, du læser online, de websites du besøger, de videoer du ser, og de ord du søger på, til hvem du kommunikerer med via e-mail, chat eller sociale medier. DPI fungerer ved at opspore og forme, hvordan beskeder bevæger sig i et netværk. De åbner og analyserer beskeder, mens disse bevæger sig i netværket, mens de identificerer dem, der kunne udgøre særlige risici. Du behøver ikke at være mistænkt for at blive påvirket af DPI – DPI opsnapper og læser enhver besked, der bevæger sig i en internetudbyders netværk.

7.1 Baggrunden for udvikling af 'deep packet inspection'

DPI blev oprindeligt udviklet for at kunne spore vira og malware (uønskede programmer), som ville kunne skade computernetværker. I dag kan man, ved hjælp af DPI ikke alene stoppe vira, men også identificere ondsindet, farlig eller kriminell aktivitet, der udfoldes via internettet.



Deep packet inspection finder sted i 'router.' En router er en enhed, der dirigerer beskeder rundt i de forskellige netværk, der tilsammen udgør internettet. Alt det udstyr, der huser den teknologi, som foretager 'deep packet inspection', er ejet af

internetselskaberne. Disse selskaber kan kontrollere, hvordan internettet fungerer lokalt, regionalt, nationalt eller internationalt. Det er de selskaber, som ejer routerne, der har været foregangsmænd for den teknologi, der foretager 'deep packet inspection.' Naturligvis ønsker selskaberne at anvende teknologien til deres egne formål, men de kan også tjene penge på at sælge deres opfindelse til andre. Andre virksomheder, blandt andet våbenkoncerner, har også udviklet DPI teknologi og ønsker at gøre det samme. Der findes nu et marked for DPI teknologi.

Sådan virker 'deep packet inspection'

Når du sender eller modtager information over internettet, gennemgår denne information en meget kompleks proces og passerer gennem adskillige computere.

Computere, der er forbundet gennem internettet, bryder den information, som du sender eller modtager, op i mindre dele, som kaldes 'pakker.' Det sker, så informationen nemmere kan bevæge sig gennem internettet. Når 'pakkerne' ankommer på deres destination, bliver de koblet sammen igen ligesom i et puslespil for at genskabe beskeden. Hver pakke har en betegnelse, som kaldes en 'header': Denne beskriver, hvad det er for en pakke, hvem den er fra og hvor den skal hen, ligesom et brev, der sendes via postvæsenet. Inde i pakken er beskedens indhold, som kaldes dens 'payload.'

Hver pakke har adskillige lag, som hver indeholder forskellige former for information om beskeden. Lagene er indlejret i hinanden, lidt ligesom en Babushka dukke. Internetudbydere bliver nødt til at inspicere nogle af beskedens pakker for at kunne levere den. For det meste behøver de bare at kigge på 'headerne' (uden på konvolutten) og ikke på 'payloaden' (indholdet) for at sikre sig, at en besked er leveret. Dette kaldes overfladisk inspektion eller 'shallow packet inspection.' I modsætning hertil indebærer 'deep packet inspection,' at alle beskedens pakker inspiceres, og at der ikke blot kigges på headerne, men også på payloaden.



Pakker inspiceres ved hjælp af computeralgoritmer, der scanner beskeder for særlige former for data. Under gennemgangen af intelligent overvågning beskrev vi algoritmerne som en række kalkulationer, der sorterer og analyserer data. De bruges også i DPI, men på en anden måde.

I DPI bliver algoritmerne programmeret til at lede efter særlige 'keywords,' ligesom når du leder efter information i en søgemaskine på internettet. Hvilke former for data, der ledes efter, afhænger af, hvem der foretager søgningen og hvorfor. De keywords, der bruges, kan relatere til kriminelle eller mistænkelige aktiviteter, til en ny computervirus eller endda til indkøb af et bestemt produkt.

7.2 Brugen af 'deep packet inspection'

I Europa er lovlig brug af DPI kun tilladt i meget begrænset omfang. For eksempel kan DPI hjælpe internetudbydere med at afværge computervira og såkaldt 'malware,' som truer med at ødelægge deres netværk. Men teknologien kan også analysere alt indhold af online kommunikation. På den måde er det muligt at anvende teknologien til at spore ulovlig internettrafik, så eksempelvis distribution af børneporno. Dette er juridisk omstridt, da den europæiske lov om opsamling af kommunikation blev lavet, før DPI eksisterede. Den eksisterende lov tillader 'filtrering' af internettrafik. For at kunne regulere brugen af DPI, er der brug for ny lovgivning på området.

Deep packet inspection må ikke finde sted i Europa, hvis datamaterialet bliver brugt af virksomheder til at målrette reklamer eller af myndigheder til at stoppe politisk følsomt indhold. DPI må heller ikke bruges i flæng, idet europæisk databeskyttelseslovgivning forbyder overvågning af kommunikation uden afsenders og modtagers samtykke.

DPI ville også overtræde Den Europæiske Menneskerettighedskonvention, hvis teknologien blev brugt på denne måde, fordi den indbefatter uvarslet, massiv, ikke-målrettet overvågning: Den kan aflæse enhver lille detalje af den information, der sendes og modtages mellem computere. Situationen er meget anderledes i USA, hvor brugen af DPI ikke er reguleret af lovgivningen, og hvor mange virksomheder bruger teknologien til at målrette reklamer. Hvis du har en Gmail™ eller Yahoo™ e-mail adresse, vil dine beskeder næsten helt sikkert bevæge sig gennem USA og dermed blive udsat for DPI.

I sommeren 2013 kom det frem, at DPI bliver brugt af såvel USA's som Storbritanniens efterretningstjenester (NSA og GCHQ) som led i deres overvågningsprogrammer.

Det er uklart, hvordan man egentlig kan spore, begrænse eller kontrollere DPI. Lovgivningen prøver desperat at holde trit med, hvad teknologien er i stand til. Det er meget vanskeligt at finde ud af, hvor omfattende brugen af DPI egentlig er. Enhver besked, du sender eller modtager, kan bevæge sig rundt over hele verden, før den ankommer. Den kan have været udsat for DPI foretaget af en internetudbyder eller af en statslig sikkerhedstjeneste i en lang række lande. Det er nærmest umuligt at vide. DPI producerer yderligere information, som kan udveksles mellem internetudbydere og myndigheder, og det er svært at vide, hvad der sker med resultaterne af DPI-søgningerne. Uden lovgivning på området befinder man sig i en 'det vilde vesten'-situation, hvor både virksomheder og regeringer kan udnytte dette juridiske tomrum.

Der er ingen tvivl om, at mange forskellige institutioner verden over benytter sig af DPI. Internetudbydere, marketingvirksomheder, politiet og nationale sikkerhedsagenturer bruger det indimellem. Der findes fem dokumenterede anvendelsesområder for DPI ud over den omfattende overvågningsaktivitet udført af NSA, der blev afsløret i sommers: De tre er kommercielle, og de to har med offentlig og national sikkerhed at gøre.

7.2.1 Kommercielle anvendelsesområder

- **Netværkssikkerhed:**
Beskeder undersøges for at sikre, at de ikke indeholder fejl eller vira.
- **Personaliserede reklamer:**
Der opsamles data fra beskeder om en persons forbrugsmæssige

præferencer. Dette er ikke lovligt i Europa, men tilladt i USA, hvor nogle forbrugere bifalder det. Det tillader dem nemt at få adgang til varer og services, der passer til deres behov.

- **Håndtering af digitale rettigheder:** Beskeder undersøges for ulovlig fildeling og brud på ophavsretten.

Kontrovers i forbindelse med deep packet inspection: Phorm og forbrugerdata i England

I 2008 forsøgte et amerikansk firma ved navn Phorm at søsætte et system i England med telefonudbydere British Telecom, Virgin Media og TalkTalk. Phorm benyttede DPI til at opsnappe brugernes vaner, når de surfede på internettet. Firmaet analyserede herefter datamaterialet og solgte det til annoncører. Internetudbydere fortalte brugerne, at dette tiltag bekæmpede cyberkriminalitet, men afslørede ikke, at de brugte informationen til at målrette reklamer. British Telecom foretog hemmelige tests af teknologien og foretog over 18 millioner dataindsamlinger. Da de engelske forbrugere fandt ud af dette, protesterede de, fordi databehandlingen var blevet foretaget uden deres samtykke. Til sidst blev Phorm teknologien opgivet af alle internetudbydere. Europakommissionen sagsøgte herefter den britiske stat for at have tilladt brugen af Phorm. Sagen blev lukket i januar 2012, efter England ændrede sin lovgivning på området til at inkludere sanktioner ved brug af uretmæssig indsamling af kommunikationsdata.

7.2.2 Offentlige og nationale sikkerhedsanvendelser

Statslig overvågning af kriminel

aktivitet: Deep packet inspection bliver set som et muligt efterforskningsværktøj i forhold til særlige forbrydelser, selvom dette er juridisk kontroversielt (og kan være ulovligt). Dette indbefatter forbrydelser:

- som begås imod computersystemer eller begås ved hjælp af en computer (for eksempel distribution af børneporno).
- hvor racistisk information er blevet delt, eller hvor der er blevet udsendt racistiske trusler.
- hvor der er blevet tilskyndet til eller organiseret terrorisme.
- hvor der er blevet delt information, der bifalder folkemord eller forbrydelser mod menneskeheden.

Censur: Det er blevet formodet, at DPI har været brugt til at fejlinformere politiske modstandere i undertrykkende regimer over hele verden. Den amerikanske forsvarsvirksomhed NARUS, som er et datterselskab af Boeing, solgte DPI til Libyen, som benyttede det til at undertrykke kritiske røster under Det Arabiske Forår. I modsætning hertil begrænsede England salget af DPI-teknologi til Egypten, Bahrain og Libyen under Det Arabiske Forår. Selvom det er uklart, hvem der er leverandør af teknologien, ved man, at Iran benytter DPI - ikke kun til at aflure og censurere, hvilken information borgerne kan få online adgang til, men også til at ændre dette indhold for bevidst at misinformere. Kina benytter DPI på en tilsvarende facon. Spørgsmålet er, hvorvidt internetbaseret censur også foregår i Europa.

7.3 Sikkerhedsforbedringer

Deep packet inspection kan forbedre sikkerheden ved at identificere og blokere skadelige, farlige eller kriminelle beskeder som beskrevet i afsnit 6.2.2

Selvom DPI ikke kan forebygge den alvorlige kriminalitet, kan teknologien hjælpe til at forbrydelsen bliver opdaget og opklaret. Desuden kan DPI forhindre at computervira og andre typer af internetkriminalitet ikke bliver spredt.

7.4 Problemer

Deep packet inspection giver anledning til følgende alvorlige problemstillinger:

1. DPI ser alt.
 - Teknologien kan analysere alle beskeder, og de følsomme data, de måtte indeholde, hvilket reelt betyder, at elektronisk kommunikation ikke længere er privat.
 - Visheden om, at kommunikation ikke længere er privat, kan måske resultere i en alvorlig 'afskrækkelseseffekt', hvor folk bliver bange for at kommunikere åbent og udtrykke sig frit.
 - Brugen af DPI bliver nødt til at være meget strengt kontrolleret, da teknologien kan give stor magt.
2. Teknologiens muligheder ændrer sig hurtigere end lovgivningen.
 - Der findes ingen klar lovgivning omkring, hvad DPI må bruges til.
 - I praksis afhænger brugen af DPI af brugerens etik. Teknologien kan bruges til alt lige fra effektiv funktionalitet i computernetværk til politisk undertrykkelse.
 - I lande hvor regeringen og de nationale kommunikationsudbydere har et tæt forhold, kan information deles så staten gives adgang til al borgernes elektroniske kommunikation

3. Det er svært præcist at udpege, hvem der bruger DPI, og hvor de gør det.
 - Databeskyttelsesmyndigheder har i længere tid efterspurgt et internationalt minimumskrav for privatliv og databeskyttelse, som kan bruges for standard for en ensartet juridisk kontrol.
 - Der bør oprettes et internationalt organ med en "DPI-kontrollør", der har tilstrækkelig magt til at kunne straffe lovovertrædere.
4. Man kan sætte spørgsmålstegn ved effektiviteten af DPI.
 - De beskeder, der bliver opfanget af DPI, som værende potentielt problematiske, er det ikke nødvendigvis. Derfor er der risiko for at beskederne misfortolkes, og at uskyldige mennesker bliver mistænkeliggjort.
 - Ekspertter har påpeget, at man ikke kan regne med, at DPI finder alt ulovligt materiale.



‘Mange af de selskaber, der benytter DPI og analyserer data om europæiske borgere, er placeret uden for Europa.

Derfor kan man ikke pålægge dem at holde op.’

Eva Schlehahn, uafhængig databeskyttelsesautoritet, Schlesvig-Holsten

8 Smartphone tracking

Da Aisha tændte sin smartphone, lagde hun mærke til, at telefonens placeringsdata viste, at den havde flyttet sig. Hun var sikker på, at der var en logisk forklaring på dette. Og det er der faktisk også, for alle mobiltelefoner har brug for at kende deres placering for at kunne fungere. Med smartphones får dette forhold helt nye dimensioner.

Smartphones har næsten overhalet schweizerkniven som det perfekte alt-i-én værktøj (og legetøj). Der findes omtrent 5 milliarder mobilforbindelser verden over. I gennemsnit er der lige knap 1,3 telefon (både almindelige mobiltelefoner og smartphones) per person i Europa. Det er et enormt antal, når man husker på, at telefoner i lommestørrelse ikke var tilgængelige før begyndelsen af 1990'erne.

8.1 Baggrunden for udvikling af smartphone tracking

Smartphones er en relativt ny opfindelse. Deres enorme popularitet skyldes, at de er i stand til at gøre mange forskellige ting ud over at være en almindelig mobiltelefon. I virkeligheden er en smartphone mere som en lille lommecomputer, der også kan foretage telefonopkald. Ligesom en stationær eller bærbar computer har de forskellige typer af smartphones også hver deres operativsystem, som muliggør e-mail, sms og søgning på nettet. Smartphones kan køre computerprogrammer, som kan levere services som spil, interaktive kort og online nyheder. De har også digitale kameraer og videokameraer, bærbare medieafspillere og store farveskærme, som kan betjenes ved berøring.

Mobiltelefonens historie kan føres tilbage til 2. verdenskrig. Grundlæggende er en mobiltelefon en trådløs radio, som kan sende og modtage beskeder. Den første trådløse radio, 'walkie-talkie', blev indført for at hjælpe

soldater med at holde kontakt med hinanden ved fronten. I 1970'erne og 1980'erne førte innovationer i mikroprocessorer til, at de første mobile mikrotelefoner så dagens lys. Den oprindelige mobiltelefon var på størrelse med en mursten og vejede ligeså meget, og dens batteri holdt kun i 20 minutter. Som tiderne dog har ændret sig! Fra 1980'erne og frem har et stadigt voksende netværk af mobiltelefonmaster forbedret telefonsignalerne både lokalt og over større afstande. Du kan måske huske, hvordan antallet af telefonmaster voksede hastigt midt i 1990'erne. Der var en heftig offentlig debat om placeringen af de uskønne telefonmaster og bekymring over, hvorvidt den forøgede stråling ville medføre sundhedsmæssige risici.

Telefonmaster er vigtige for at kunne lokalisere mobiltelefoner. En telefonmast dækker et fastlagt geografisk område. For at kunne forbinde sig til netværket,



foretage opkald og sende sms'er må alle mobiltelefoner registrere sig via den nærmeste telefonmast. En telefons placering bliver altid registreret af den mast, som den er forbundet til. Hvis den person, der benytter telefonen, flytter inden for rækkevidde af en anden telefonmast, forbinder telefonen sig til denne i stedet. På denne måde kan en persons

bevægelsesmønster spores af telefonudbyderen. Ifølge den en nuværende lovgivning i EU skal data fra telefonmaster gemmes i seks til 24 måneder. Selvom en dom fra EU-domstolen har afvist dette direktiv i april 2014, er de nationale lovgivninger endnu ikke blevet ændre. Smartphones kan også lokaliseres på andre måder. Den person, der benytter telefonen, kan indstille den, så telefonen registrerer sin position ved hjælp af GPS og ved at forbinde sig til trådløse netværk. Dette har ført til en enorm stigning i anskaffelsen af 'stedbaserede services' til smartphones.

Disse er almindeligvis tilgængelige som applikationer ('apps'), der kan installeres på telefonen. En app er et computerprogram, der kan tilbyde en særlig funktion eller service. Stedbaserede apps kan sætte brugeren i stand til at finde information om restauranter eller butikker i nærheden, eller fortælle hvilke af vennerne der befinder sig tæt på. Stedbaserede spil er nu også tilgængelige. I det hele taget vil stedbaserede services sandsynligvis være den hurtigst voksende smartphone-funktionalitet i de kommende år.

Sådan virker smartphone tracking



Både almindelige mobiltelefoner og smartphones kan trackes eller spores. Der er tre måder at spore en mobiltelefon på: telefonmaster, GPS eller trådløse netværk. Førstnævnte gælder for alle mobiltelefoner, hvorimod de to andre kun gælder for smartphones.

Mobiltelefonmaster: Alle telefoner registreres af den nærmeste mobiltelefonmast, så opkald, sms'er og e-mails kan sendes og modtages over mobilnetværket. Hver telefon indeholder et unikt referencenummer, som forbinder telefonen til en konto hos mobiltelefonselskabet og således hos brugeren. Dette muliggør oprettelsen af en brugerpakke, der passer til brugerens behov og genererer telefonregningen. Hvis sikkerhedsagenturer eller politi forsøger at spore en bestemt persons bevægelsesmønster på et bestemt tidspunkt, kan de kræve at få adgang til telefonmastdata fra mobiltelefon-selskaberne. Telefonmast-dataene indikerer, hvorvidt personens telefon var inden for rækkevidde af en bestemt telefonmast. Når sådanne data er gennemgået fra et antal forskellige master, kan telefonens placering spores, og dens brugers bevægelsesmønster fastlægges.

GPS: Smartphones indeholder landkort og applikationer, som fungerer via GPS. Når GPS-funktionen i en smartphone er slået til, fastlægger telefonen sin placering på jorden ved at beregne, hvor langt væk den er fra den nærmeste GPS-satellit ude i rummet. Når funktionen er slået fra, kan telefonen ikke lokalisere sig selv via GPS. Funktionen kan dog slås til, uden at brugeren bliver advaret. Det bruges blandt andet til at finde stjålne eller bortkomne telefoner. App-udbydere indsamler disse placeringsmæssige data, og nogle sælger dem videre til reklameformål. Hvis sikkerhedsagenturer eller politi er i gang med at spore en bestemt person, kan de kræve at få adgang til telefonselskabernes GPS-data.

Trådløst: Smartphones kan forbinde sig til trådløse netværk, der fungerer inden for et bestemt område. Når telefonen forbinder sig til et trådløst netværk, kan den lokaliseres inden for dette netværksområde. Hvis funktionen slås fra, vil det ligesom med GPS-funktionen betyde, at telefonen ikke kan spores via denne teknologi. Et WiFi access point vil typisk have en rækkevidde på 20 meter indendørs og en større rækkevidde udendørs.

Andre 'intelligente' mobile personlige apparater såsom iPads, tablets og notebooks kan spores på samme måde.

Stedbaserede services har meget at tilbyde smartphone-brugeren. Men nogle fortalere for beskyttelse af privatlivet er bekymrede over den information, som kan afsløres gennem smartphone tracking. For eksempel forsøgte politikerne Malte Spitz fra partiet De Grønne i Tyskland at få adgang til de placeringsmæssige data, som gennem seks måneder var blevet akkumuleret via hans mobiltelefonbrug, men han blev nødt til at sagsøge telefonselskabet for at få materialet udleveret. Da han først modtog disse data, lignede de en meningsløs strøm af tal og bogstaver. Men da Malte Spitz fik en statistiker til at se på dataene, tegnede der sig et detaljeret billede af hans liv. I samarbejde med avisen Die Zeit producerede Malte Spitz en animation, som nøjagtigt viste, hvor han havde været i løbet af et halvt år. Malte Spitz var meget bekymret over, at man så detaljeret kunne afsløre hans gøren og laden, især hvis informationen om mobiltelefonens placering blev kombineret med information fra sociale medier som Twitter eller Facebook.

For nylig påpegede dommeren i en sag i den amerikanske Højesteret, *United States v. Jones*, at GPS-data kunne afsløre 'ubestrideligt personlige' forhold som 'Besøg hos psykiateren, plastickirurgen, abortklinikken, aids-behandlingscenteret, stripklubben, forsvarsadvokaten, hotellet, hvor man lejer sig ind på timebasis, fagforeningsmødet, moskéen, synagogen eller kirken, baren for homoseksuelle osv.'

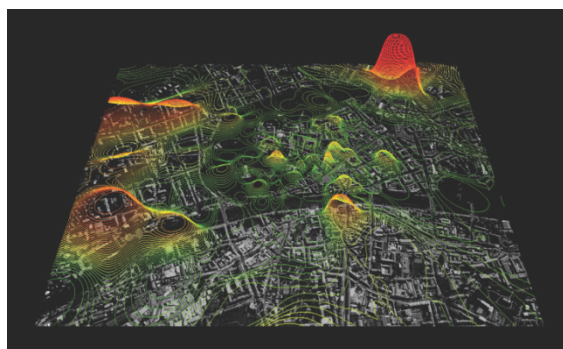
- **Personaliserede reklamer:** Softwarevirksomheder, der producerer apps som for eksempel Twitter, Angry Birds eller FourSquare, indsamler placeringsmæssige data og andre kontaktdata fra telefoner og sælger dem til annoncører. Annoncørerne bruger herefter materialet til at designe reklamer for produkter, der sælges de steder, som de nu ved, de forskellige slags forbrugere benytter. Angry Birds er for eksempel blevet downloadet en milliard gange verden over. Brugerne var overraskede over at opdage, at spillets finske udviklere, Rovio Entertainment Ltd, rutinemæssigt indsamlede og solgte spillernes placeringsmæssige data. 50 % af alle apps indsamler placeringsmæssige data, selv når app'en ikke behøver denne information for at fungere.
- **Byplanlægning:** Placeringsmæssige data kan bruges til at kortlægge, hvordan byens rum benyttes. Eftersom der er flere telefonmaster i byerne i forhold til ude på landet, kan telefoner spores langt mere nøjagtigt i byen. Dette temmelig uhyggeligt udseende billede er et kort over mobiltelefonbrug i Graz i Østrig. Forskere på Massachusetts Institute of Technology (MIT) sporede anonymt mobiltelefoner for at skabe et billede af, hvordan folk bevægede sig rundt i byen Graz. Deres mål er at skabe viden om, hvordan byen benyttes, til gavn for by- og transportplanlæggere.

8.2 Brugen af smartphone tracking

Placeringsmæssige smartphone data bliver brugt både kommercielt og i sikkerhedsmæssig henseende.

7.2.1 Kommercielle anvendelsesområder

- **Administration af telefonregninger:** Mobiltelefonselskaber har brug for placeringsmæssige data såvel som telefonens identifikationsnummer for at kunne udskrive en telefonregning.



Kort over mobiltelefonbrug i Graz, Østrig

7.2.2 Offentlige og nationale sikkerhedsanvendelser

- **Eftersøgning af forsvundne og tilskadekomne:** I USA og Canada findes der en service ved navn E-911, som forpligter til brug af GPS i alle mobiltelefoner, så de (og deres brugere) kan lokaliseres i tilfælde af en nødsituation. I Europa foretages der omkring 180 millioner nødopkald om året. 60-70 % af disse nødopkald kommer fra mobiltelefoner. Telefonen afslører selv hvor den befinder sig, når der ringes op til det Europæiske nødopkaldsnummer 112. I modsætning til amerikanere og canadiere behøver europæere ikke at have GPS slået til på deres telefon.
- **Sporing af mistænkte:** Sikkerhedsagenturer og politi kan få adgang til placeringsmæssige data ved at indsende dataanmodninger til mobiltelefonselskaber. I dag vil enhver anmodning af denne type blive behandlet under databeskyttelseslovgivningen. Når mobiltelefonselskaberne modtager en sådan anmodning, er de forpligtet til at udlevere alle tilgængelige data, der har med den mistænkte at gøre. Sikkerhedsagenturer har også andre metoder til at spore telefoner, som kan benyttes over for særligt udpegede individer.
- **Sporing af familiemedlemmer:** Andre mennesker kan også nyde godt af stedbaserede services. Mange forældre kender for eksempel til diverse mobiltelefon-sporingsværktøjer, som gør dem i stand til at vide, hvor deres børn opholder sig på alle tidspunkter af dagen.

Kontrovers i forbindelse med smartphone tracking

I kølvandet på Occupy Wall Street-demonstrationerne i New York blev Twitter tvunget til at udlevere placeringsmæssige data til de amerikanske myndigheder, så man kunne identificere demonstranterne. For nylig lancerede Twitter en ny service ved navn 'Please Don't Stalk Me', der tillader brugerne, via Google Maps, at angive et hvilket som helst sted på jorden som deres placering og indlejre disse falske data i deres tweets. Andre apps såsom 'My Fake Location', 'Fake GPS Location' og 'GPS Cheat' gør det samme.

8.3 Sikkerhedsforbedringer

Smartphone tracking forbedrer sikkerheden på en række områder:

1. Den gør det muligt for folk i farlige situationer at blive fundet og hjulpet.
2. Den gør det muligt for børn og udsatte personer at blive overvåget af deres familier.
3. Politi og retsinstanser kan benytte placeringsmæssige data til at spore individer i forbindelse med et gerningssted eller udelukke dem som mistænkte. De kan også spore mistænkte under igangværende efterforskninger.

8.4 Problemer

Smartphone tracking er forbundet med følgende problemstillinger i tilknytning til privatliv, kontrol og menneskerettigheder:

1. Brugere har ikke fuld kontrol over den information, som telefonen udsender. Dette er især problematisk for mere udsatte brugere, for eksempel vidner under beskyttelse, som måske ikke har lyst til at dele deres placeringsmæssige data, men alligevel gerne vil have fordelene ved at bruge en mobiltelefon. Nogle telefoner, såsom Apples iPhones, lagrer automatisk placeringsmæssige data i telefonen, og denne funktion kan ikke slås fra.
2. Nogle apps samler placeringsmæssige data, selvom app'en ikke har brug for disse data for at fungere. Medmindre der opstår et meget stærkt pres fra offentlighedens side, er selskaberne ikke tilbøjelige til at indrømme forbrugerne en bedre kontrol over deres placeringsmæssige data.
3. Mange app-udviklere befinder sig uden for Europa og er således ikke underlagt europæisk databeskyttelseslovgivning. Derfor er det også vanskeligt for EU at kræve, at apps'ene skal være mere privatlivsvenlige. En nylig tilføjelse til EU's ePrivacy-direktiv kræver imidlertid, at brugere skal have mulighed for at give deres samtykke til, at data fra deres smartphone apps behandles, uanset hvor i verden app'en er baseret.
4. I lande, hvor myndighederne og mobiltelefonudbydere har et tæt forhold, kan information deles på en måde, som giver staten adgang til alle borgernes placeringsmæssige data – meget lig tilfældet med deep packet inspection.
5. Eftersom placeringsmæssige data har været brugt til at identificere demonstranter, kan brugen af sådanne data potentielt have en 'afskrækkende effekt', hvor folk bliver varsomme med at protestere og udøve deres demokratiske rettigheder.



‘Smartphone tracking giver både folk muligheder og holder dem under opsyn. Teknologien kan levere en række services og forbedre sociale relationer ... men interesserne forbundet med deling af placeringsmæssige data er ikke altid lige indlysende eller lige nemme at styre.’

Gus Hosein, Privacy International

9 Biometri

'Biometri' kan både referere til systemer der bruger målbare fysiske karakteristika af en person, som eksempelvis fingeraftryk, DNA, iris scanner, ansigts struktur, kropslugte eller til analyse af personspecifikke adfærdskarakteristika, så som analyse af gangart, stemme eller tasteanslag, med det formål at kategorisere eller verificere den påstående identitet af en person.

Nogle lande tager deres borgeres fingeraftryk og andre målbare fysiske karakteristika og opbevarer dem i ID-kort eller i en database. I disse tilfælde er der tale om at en persons karakteristika bliver opbevaret i et biometrisk system. På et senere tidspunkt bliver en persons biometriske information sammenlignet med anden information som blev registreret på samme tidspunkt, og herved kan personens identitet blive verificeret. Betydelige teknologiske fremskridt indenfor databehandling har resulteret i et automatiseret biometrisk system, der blandt andet muliggør identitetstjek af store menneskemængder på få sekunder.

9.1 Baggrunden for udviklingen af biometri

Udviklingen af nationale retssystemer i 1800-tallet, medførte behov for formaliserede måder at identificere borgere på. Retssystemerne havde til hensigt at straffe første-gangs-lovovertredere mildt, og vaneforbrydere strengere. Det blev derfor nødvendigt med et system der kunne registrere en persons lovovertrædelse sammen med et målbart fysisk karakteristika. I Frankrig udviklede Alphonse Bertillon "Bertillonage" eller antropometri, dvs. metoder til identifikation af en person baseret på detaljerede opmålinger af deres kropslige dimensioner, f.eks. højde, armlængde, fysiske beskrivelser og fotomateriale. I 1890'erne udvikledes en mere lovende tilgang, da Sir Francis Galton udviklede en metode til at identificere kriminelle ud fra deres fingeraftryk. Sammenlignet med Bertillons målinger, var denne metode mere

individualiseret. I 1900-tallet blev andre biometriske kendetegn opdaget som potentielle identifikationsmetoder. I 1936 foreslog Frank Burch at anvende det unikke mønster i menneskeøjets iris, og i 1960'erne blev teknikker for ansigts- og stemmegenkendelse udviklet.

9.2 Brugen af biometri

Biometri er traditionelt set blevet anvendt af myndigheder til at identificere kendte og ukendte kriminelle, eller til at sikre at adgang til regeringsbygninger og andre steder med høj sikkerhedsprofil, udelukkende gives til de rette vedkommende.

Siden årtusindeskiftet, er biometri i stigende grad blevet brugt ved grænsekontroller. Biometriske data er registreret på rejsende der ønsker adgang til særlige lande. Ved ankomst, sammenlignes de registrerede data med informationer i en database, for at verificere om den rejsende tidligere er blevet nægtet indrejse, er en identificeret sikkerhedsrisiko, eller tidligere har opholdt sig i landet uden gyldigt visum.

Eksempelvis indsamler EU 10 fingeraftryk og et digitalt fotografi af personer der ansøger om visum. Disse biometriske data er opbevaret i den såkaldte VIS-database (Visa Information System). EU har oprettet det tilsvarende EURODAC, en stor database med fingeraftryk fra asylansøgere og dokumentløse migranter der har opholdt sig inden for EU. Databasen er med til at effektivisere overholdelsen af de krav der er ifølge Dublin Konventionen er til behandling af asylsager

I militær kontekst, bruger det Amerikanske Militær, i Afghanistan og Irak, små mobile og håndholdte enheder der muliggør biometriske målinger, som f.eks. iris scanning. Personer med en særlig interessant profil bliver noteret i et digitalt biometrisk system, der muliggør at soldater i felten kan verificere identiteter, f.eks. af personer mistænkt for at terrorisme eller for at afsløre om en person har tætte forbindelser til voldelige oprørsgrupper. Databasen indeholder p.t. data på 209.000 personer verden over.

Selvom biometri originalt er blevet udviklet af sikkerhedsmæssige hensyn, er metoden gennem 1900-tallet i stigende grad blevet brugt i erhvervslivet som kontrolmekanisme i forbindelse med adgang. Modsat nøgler og kodeord, er de personlige fysiske kendetegn svære at miste eller glemme. Samtidigt er de biometriske data svære at kopiere. Af disse grunde, mener mange mennesker at biometri er sikrere at anvende end nøgler og kodeord. Eksempelvis har Apples nyeste Iphone en sensor der kan scanne brugerens fingeraftryk. Facebook anvender ansigtsgenkendelsesværktøjer til automatisk at foreslå identiteter på personer på billeder. Forskningsprojektet DeepFace har slået fast at teknologien med 97,25% sikkerhed kan afgøre om to billeder har det samme ansigt. Nogle banker er i gang med at udvikle biometriske systemer der genkender stemmer, til at sikre at kunder ved at fremsige et kodeord, kan få adgang til bruge kredit kort og foretage betalinger på deres mobiltelefon. Nogle firmaer bruger bærbare computere som inkluderer fingeraftryksscannere til at sikre at adgang kun gives til de rette personer. Digitale reklameskilte i det offentlige rum, kan også vise forskellige reklamer afhængigt af personen der beskuer det, f.eks. bestemt ud fra alder eller køn. Dog bliver biometri i stigende grad brugt, ikke kun som værktøj til at identificere personer, men også til adfærdsanalyser.

Adskillige smartphone fitness-app's bruger real-tid biometri, som f.eks. hjerteslag og åndedræts hastighed til at give detaljerede brugerspecifikke anbefalinger. Inden for sikkerhedsbranchen anvendes nye teknologier med biometri sammen med allerede eksisterende teknologier, f.eks. ansigtsgenkendelse sammen med avancerede overvågningskameraer, som giver nye og mere vidtrækkende overvågningsmuligheder. I denne kontekst er det vigtigt at bemærke, at nye biometriske systemer har potentiale til at indsamle informationer, både på afstand og i bevægelse, uden at kræve tilladelse fra individet som registreres. Disse systemer kan igangsætte et alarmsystem, f.eks. når et avanceret overvågningskamera identificerer en kendt kriminel hvis billede allerede er registreret i politiets database.

9.3 Sikkerhedsforbedringer

Biometri kan forbedre sikkerhed på følgende måder:

Identifikation af biometriske indikatorer har været brugt i over 100 år til ordenshåndhævelse til både bekræftelses- og identifikationsopgaver. Systemer der kan analysere en persons ansigt samt systemer til at analysere en persons DNA kan bidrage meget effektivt til at bekæmpe kriminalitet og effektivt afsløre identiteten på en ukendt person der mistænkes for alvorlig forbrydelse.

Sådan virker biometrisk identifikation

Det første skridt er at skaffe en biometrisk prøve, for eksempel et fingeraftryk eller en iris scanning, typisk i form af et billede. Dataene kan gemmes enten som billede, eller som en skabelon, hvilket er en digital repræsentation af det biometriske, lavet ved hjælp af en algoritme. For at sikre højest mulig grad af privatliv, anbefales det kun at gemme skabelonen og slette det originale billede.

Det biometriske data, enten billedet eller skabelonen, kan gemmes forskellige steder, for eksempel der hvor en optagelse er fundet sted (f.eks. i en læser) til senere brug, og på et apparat som individet bærer på (f.eks. et 'smart cart'). Det kan også sendes til og gemmes i en centraliseret database der er tilgængelig via et eller flere biometriske systemer.

Når et biometrisk system tilgås, vil det bede vedkommende der prøver at tilgå det om at forelægge de biometriske karakteristika. Systemet vil så sammenligne det forelagte billede eller skabelon med det biometriske data der er gemt om personen i systemet.

Hvis biometri sammenligningsprocessen er succesfuld, genkender og godkender systemet personen. Hvis matchet ikke lykkes, bliver personen ikke genkendt og dermed afvist. Det billede eller den skabelon der skabes når biometrien første gang optages, vil sjældent være identisk til det billede eller den skabelon af biometrien som personer senere præsenterer for læseren. De relevante træk ændres ofte lidt eller forelægges på en lidt anden manér end under registreringen. Derfor vil der uundgåeligt være en grad af sandsynlighed i sammenligningen.

Indsamlingen af biometri kan bruges til at øge sikkerheden af specielt følsomme databearbejdningsprocesser. De kan for eksempel hjælpe med at sikre at det kun er autoriserede personer hos et specifikt teleselskab der har adgang til trafik data (og placeringsdata) som skal gemmes til myndighedsudøvelsesformål.

9.4 Problemer

Adskillige ulemper bør overvejes:

1. Biometrisk data er ikke ufejlbarligt.

- Det kan siges at to digitale optagelser af biometriske træk aldrig vil være helt ens. Forskelle i typen af udstyr brugt til registrering eller forskellige omgivelser (lys, temperatur) kan forårsage forkerte godkendelser og afvisninger: et biometrisk system kan identificere en person forkert eller fejlagtigt ikke afvise en bedrager. En forkert afvisning sker når et individ ikke sammenlignes med sin egen eksisterende biometriske skabelon.
- Endvidere ændrer de biometriske træk sig for nogen i løbet af deres livstid, for eksempel grundet aldring, operationer eller ulykker. Et biometrisk system vil muligvis ikke kunne genkende en sådan person.
- Forfalskninger af biometrisk data er muligt, hvilket resulterer i en øget mulighed for identitetstyveri.
- I sit nuværende udviklingsstadium er det stadigvæk relativt let at snyde f.eks. et ansigtsbiometrisk genkendelsessystem ved hjælp af simple ændringer i udseende som forskellige frisurer, skæg, make-up, briller, kontaktlinser, osv.

2. Før i tiden var biometri dyrt og tidskrævende. På grund af disse begrænsninger var indflydelsen på den enkeltes datasikkerhedsrettigheder begrænsede. Dette har nu ændret sig,

og det kan lede til genetisk diskrimination og gradvist tab af privatliv hvis der ikke implementeres tilstrækkelige sikkerhedsforanstaltninger. For eksempel kan udstyringen af videoovervågning og smartphones med ansigtsgenkendelsessystemer gøre en ende på anonymitet og sporløs færden for individer.

- ### 3. I de fleste tilfælde kræver registrering personlig deltagelse fra individet, for eksempel når der tages fingeraftryk, og det kan fungere som en passende mulighed for at informere og bekendtgøre om retfærdig behandling af data. Men det er også muligt at registrere individer uden deres vidende eller samtykke, for eksempel ved brug af overvågningskamarasystemer med indbyggede ansigtsgenkendelsessystemer. Dette har alvorlige konsekvenser for deres muligheder for at udøve deres ret til samtykke eller bare at få information om behandlingen af deres data.
- ### 4. Biometri som uforanderlige karakteristika kan også være problematisk så snart registreringen i sig selv er kompromitteret, da det potentielt kan lede til falsk stigmatisering af et individ.

10 Er teknologien den eneste løsning?

Du undrer dig måske over, hvorvidt sikkerhedsteknologier er den eneste løsning på sikkerhedsproblematikker. Til tider virker det som om, sikkerhed ikke går ud på andet end at spore og identificere mistænkte i den brede befolkning. Overvågningsbaseret sikkerhedsteknologi arbejder ud fra den antagelse at et udvidet overvågningssystem der overvåger så mange så muligt så præcist som muligt er den bedste måde at opdage potentielle trusler og identificere potentielle kriminelle efter forbrydelsen er blevet begået, eller, alternativt, endda før forbrydelsen er blevet begået. Når sådanne teknologier implementeres, søges øget sikkerhed næsten udelukkende gennem øget overvågning.

Det er til dels rigtigt, men det er ikke hele historien. Mens sikkerhedsteknologier bliver brugt til at finde kriminelle og terrorister, samt prøve at forudsige deres næste træk, så eksisterer der også andre strategier til at forbedre sikkerhed ved andre midler. I dette kapitel eksemplificerer vi andre tilgange der kan overvejes som alternative sikkerhedsforanstaltninger.

Sikkerhed er et tvetydigt, socialt (normativt?) begreb der kan opfattes på forskellige måder. Forhold vedrørende samfundsmæssig stabilitet, social sikkerhed eller –pålidelighed, for at nævne blot nogle få eksempler, er i høj grad forbundet med det følte niveau af sikkerhed.

10.1 Alternative sikkerhedsforanstaltninger: på globalt niveau

EU's sikkerhedsprioriteter, som vi så på tidligere, vidner om, at sikkerhed er noget, der griber ind i alle områder af livet. De drejer sig om de 'klassiske' sikkerhedsproblematikker såsom kriminalitet og terrorisme. Ud fra hvad vi har set på de foregående sider, er det muligt at anvende de nye sikkerhedsteknologier til at finde de mennesker, som er involveret i sådanne aktiviteter. Men der er også underliggende problemer, der er årsag til, at sådanne sikkerhedsproblematikker overhovedet opstår – fattigdom, nationale eller internationale konflikter, politiske og religiøse forskelle. Sikkerhedsteknologier kan ikke gøre noget ved sådanne grundlæggende årsager.

EU's sikkerhedsprioriteter henviser også til kriser og katastrofer som sikkerhedsproblematikker. Disse katastrofer kunne involvere fødevare- eller vandmangel, økonomiske kriser, epidemier eller naturkatastrofer: forhold, der udfordrer den overordnede menneskelige sikkerhed.

Når vi taler om sikkerhed som 'overordnet menneskelig sikkerhed' er det også nødvendigt kort at kigge på nogle globale samfundsmæssige udfordringer:

Sikkerhedsinitiativer der søger at øge sikkerhedsniveauerne i forhold til natur- eller menneskeskabte katastrofer kan, i nogen grad, foreslås og implementeres. Sådanne initiativer har ofte rod i langsigtede, omfattende metoder. Fremme af globale systemer til retfærdig handel, nødhjælp og gældsafvikling, for eksempel, prøver ikke bare at adressere økonomiske forhold men også miljømæssige problemer relateret til udtømmning af naturressourcer, forurening og voldsomme forandringer i miljø- og klimacyklusser. Disse er i sidste ende sikkerhedsproblemer. Ligeledes er politiske beslutninger, der skal forbedre lokale og nationale nødhjælpsberedskabsplaner, eller forbedre kommunikation og informationsinfrastruktur, så vel som mad og vand forsyninger, alternative midler til at forbedre leveforhold, og dermed øge sikkerhedsniveauerne i relevante områder.

Forskellige måder at forstå sikkerhed på, og dermed forskellige måder at fremme det, har udviklet sig, ikke bare på globalt plan. Derfor vil vi gerne henlede din opmærksomhed på dine lokale omgivelser for at forestille dig en række andre metoder der prøver at øge sikkerheden.

Hovedpointer: nationale og internationale løsninger:

- Fremme af retfærdige globale handels-, nødhjælps-, og gældsafviklingssystemer.
- Fremme af økonomisk og social lovgivning for at skabe mere ligelig fordelt indkomst og ansættelse.
- Forbedring af nødhjælpsberedskabsinfrastruktur og –ressourcer.
- Brug af vedvarende- og alternative energikilder på mere effektiv vis.
- Forbedring af kommunikations- og informationsinfrastruktur, samt mad- og vandforsyninger i de dele af verden hvor der er brug for det.

10.2: Alternative sikkerhedsforanstaltninger: det lokale niveau

Der forskellige måder at forstå og opnå højere sikkerhedsniveauer på lokalt niveau. For eksempel kan sikkerhed tilstræbes via implementering der ikke involverer overvågning. Metaldektorer, bevægelsesfølsomt lys, lyd-niveaualarmer, generelle advarselsmekanismer, eller endda offentlige nødtelefoner, er alle teknologier der sigter til at øge sikkerheden uden at introducere overvågning eller dataindsamling. Derimod forsøger de at øge folks muligheder for at reagere og intervenere for at beskytte sig selv og deres ejendom. Alternativt kan teknologier som metaldektorer hjælpe offentlige autoriteter med at opdage potentielle farer ved at fokusere på kilde for truslen (her, metalobjektet) frem for personlige karakteristika der potentielt udgør en trussel. De kan være meget effektive men er begrænsede til det specifikke sted og øjeblik i hvilket de opererer. Men de udgør ikke en trussel i forhold til privatlivets fred eller overvågning.

Forsøg på at forhindre kriminalitet og øge sikkerhed i offentlige rum kan også bestå i administration og planlægning af byrum. Strukturelle ændringer for at fremme et sikrere bymiljø, for eksempel i ved at reducere 'fareområder' (gader, pladser og parker der er svært overvågelige), kan være med til at øge den fornemmede følelse af sikkerhed i offentlige heden, og på samme tid, hjælpe borgere med at blive mere opmærksomme på deres omgivelser og de farer der kan opstå.

Hovedpointer: metoder der ikke er baseret på overvågning og dataindsamling:

- Kriminel prævention gennem byplanlægning og miljøindretninger.
- Implementering af teknologier der ikke involverer overvågning.

Det er også muligt at introducerer sikkerhedsforanstaltninger der søger øgede sikkerhedsniveauer gennem overvågning men som ikke nødvendigvis involverer sikkerhedsteknologier der medfører massiv dataindsamling og -lagring. Et typisk eksempel kunne være at styrke politiets aktiviteter ved for eksempel at øge lokale patruljeringer. Traditionelle politiaktiviteter søger også at øge

sikkerhedsniveauer ved brug af ikke-teknologisk overvågning. Desuden eksisterer der nabohjælpsprogrammer der fungerer ved at beboere i et beboelseskvarter distribuerer patruljering imellem sig, hvor de undersøger mistænkelig adfærd i området og rapporterer det til det lokale politi. Identitetstjek ved brug af gæstelister udarbejdet på forhånd for at regulere adgang for folk til offentlige eller private områder, udført af dørmænd eller sikkerhedspersonale, er andre eksempler på sikkerhedsforanstaltninger der baserer sig på overvågning for at øge sikkerheden uden at involvere teknologi eller massiv dataindsamling

Hovedpointer: ikke-teknologiske metoder til at øge overvågning

- Styrkelse af traditionelt politiarbejde.
- Implementering af naboværn og lignende.
- Ansættelse af menneskelige gatekeepers, for eksempel sikkerhedspersonale eller dørmænd.

Endelig er det måder at adressere sikkerhed som søger at øge sikkerhed, ikke så meget gennem undertrykkelse af kriminelle aktiviteter eller truende afskrækkelse, men gennem en langsigtet, grundig tilgang der kan adressere de underliggende sociale og økonomiske årsager til vold, kriminalitet, religiøs had, racisme eller social diskrimination. Også her er sikkerhedsteknologier mindre effektive til at adressere disse mere langsigtede og komplekse menneskelige sikkerheds-problemer.

Efter denne bredere forståelse af sikkerhed, er der lavet forskellige lovgivningsmæssige forslag, såsom at etablere bedre relationer mellem lokalsamfund og politi eller at involvere tros-eller andre samfundsgrupper i at administrere problemer lokalt for at øge den sociale tillid og sammenhængskraft. At øge den sociale og økonomiske støtte gennem aktive beskæftigelses politikker, samt trænings- og mentor muligheder for dem der er i høj risiko for at blive involveret i kriminalitet, er også, dybest set, sikkerhedsforanstaltninger. Frivillighedsforeninger til rehabilitering af mennesker med alkohol eller stofmisbrug, implementering af velkomstcentre for migranter eller etablering af, ofte selv-organiserede, social centre er også eksempler på hvordan man med lokale midler til at øge social sammenhængskraft samtidig kan øge sikkerheden i et givent område.

Den grundlæggende idé bag disse tilgange til sikkerhed er to-fold af natur: på den ene side handler det om aktiv deltagelse fra dem der er bekymrede (altså de lokale borgere) i at løse konflikter og på den anden side, samtidig søge at (re)integrere ballademagerne eller lovovertrædere gennem socialt samfundsarbejde frem for disciplinær straf.

Aktiv uddannelses politikker rettet mod integration, selv-styring og respekt for gensidig diversitet kan medvirke til at reducere sociale, kulturelle og økonomiske spændinger og til at forbedre følelsen af at høre til et lokalt og nationalt fællesskab indirekte ved at bidrage og dermed øge sikkerhedsniveauet.

Hovedpointer: metoder der er direkte rettet mod samfundsmæssige forhold og reduktion af risiko på lang sigt

- Investering i sociale virkemidler, midler og personale.
- Næring af aktiv borgerdeltagelse til at løse lokale problemer og konflikter.
- Etablering af bedre lokalsamfundsrelationer med forskellige interessentgrupper.
- Øgning af (økonomisk) støtte til beskæftigelsespolitik, videreuddannelsesmuligheder og lignende.
- Implementering af velkomstcentre, naboværn centre og sociale centre

Vi har kort introduceret alternative metoder og koncepter i dette kapitel, men du har muligvis nogle andre og anderledes ideer om hvordan sikkerhed kan forbedres. Eller måske synes du at Europas sikkerhedsfokus skulle flyttes fra kriminalitet og terror til andre områder.

Sikkerhedsteknologier kan altså bruges til at finde kriminelle og terrorister og forudse deres næste skridt, men der er også andre løsninger. Du kan se nogle af dem herunder. Måske har du også dine egne forslag til, hvordan sikkerheden kan forbedres, eller det kan være, at du synes, at det europæiske sikkerhedsfokus skal flyttes væk fra kriminalitet og terror, for at prioritere andre områder højere.

10.2 Lokale løsninger

- > Fremme et mere trygt nærmiljø gennem forbedret gadebelysning, offentlige nødtelefoner og øget tilstedeværelse af politi i gaderne
- > Skabe bedre relationer mellem lokalsamfund og politi gennem kriminalitetsforebyggende tiltag
- > Tilskynde trossamfund og andre sociale grupper til at løse deres problemer lokalt for at styrke den gensidige tillid i samfundet
- > Etablere gennemsigtigt og ansvarligt lokalstyre og lokalpoliti
- > Skabe rig mulighed for ansættelse, uddannelse og mentorordninger for dem, der er i risikogruppen for at blive involveret i kriminalitet.

8.2 Nationale eller internationale løsninger

- > Befordre retfærdige globale handelsrelationer, hjælperelationer og gældssanering
- > Forbedre nødhjælpsinfrastrukturer og nødressourcer
- > Forbedre drikkevandet og kommunikationsinfrastrukturen samt fødevareforsyningen i de dele af verden, der har brug for det
- > Udnytte bæredygtige og alternative energikilder mere effektivt
- > Løse problemer med ulighed og diskrimination.

9 Og nu er det din tur...

Vi håber, at du ikke føler dig alt for overvældet af information på nuværende tidspunkt! De gode nyheder er, at du nu er nået til vejs ende i hæftet og kan bruge noget tid på at tænke og reflektere over de problemstillinger, vi har opridset.

Vi har skitseret de fem sikkerhedsteknologier, som vi skal diskutere på borgertopmøderne. Vi har forklaret, hvordan de virker, hvordan de bliver brugt, hvilke sikkerhedsforbedringer de tilbyder, og de problemer, som opstår i deres kølvand. Vi har også beskrevet den kontekst, som teknologierne blev udviklet i; nemlig et Europa, som er meget optaget af sikkerhed, og hvor sikkerhed er en del af hverdagslivet. Problemet med overvågning og privatliv er også fremtrædende på grund af den blotte mængde af personlige data, som nu benyttes i sikkerhedskontekster. Endelig kastede vi et blik på alternative, ikke-teknologiske tilgange til at styrke sikkerheden i samfundet.

Det er nu op til dig at overveje din holdning til disse problematikker. Hvis disse teknologier rutinemæssigt blev benyttet i sikkerhedsmæssig henseende, hvor acceptable ville de så være? Du føler måske, at teknologierne, på hver deres måde, er effektive i forhold til at øge sikkerheden og potentielt kan reducere kriminalitet. Men du føler måske også, at alternative, ikke-teknologiske løsninger ville være bedre. Det kan være, at du synes at mere traditionelle løsninger, hvor man for eksempel har professionelt trænet sikkerhedspersonale og politi skulle bruges i højere grad end udbredt overvågning af information. Måske mener du,

at sikkerhed slet ikke er et problem, og at vi ikke bør bekymre os så meget om det.

På samme måde er du måske overbevist om, at disse teknologier er i trygge hænder, fordi de anvendes af statslige institutioner, som er offentligt ansvarlige. Eller måske tvivler du på, om disse autoriteter er i stand til at anvende sikkerhedsteknologierne på en kompetent, etisk forsvarlig måde til alles bedste.

Måske synes du, at teknologierne ikke rigtig har noget med dig at gøre: De er trods alt rettet mod andre, som har gjort noget galt, og de bliver brugt på steder og områder, hvor du ikke kommer. Men det kan også være, du føler, at alle burde bekymre sig om disse problematikker på grund af den store mængde data, som teknologierne behandler, og fordi de gør enhver til en potentiel mistænkt. Måske er du tryk ved, hvordan sikkerhedsteknologierne bruges i dag, men bekymret over, hvordan de kan blive brugt i fremtiden.

Uanset hvad man mener, vil det for de fleste være alt andet end ligetil at afveje hensynet mellem privatliv og sikkerhed. SurPRISE stræber mod at forstå de forskellige holdninger, folk indtager, i forbindelse med de nye sikkerhedsteknologier.

Vi glæder os til at se dig på borgertopmødet om et par uger. Hvis du har lyst til at vide mere om projektet og dets partnere, kan du besøge SurPRISEs website på:

<http://surprise-project.eu>

’Privatlivsrelaterede problemer er lige dele politiske og lovgivningsmæssige problemer da de er juridiske og teknologiske af natur.’

Colin J. Bennet, professor og sikkerhedseksport hos Department of Political Science, University of Victoria, Canada.

Om dette informationshæfte

Dette informationshæfte er skrevet for at informere de borgere, som deltager i SurPRISE projektets borgertopmøder. Publikationen er tilvejebragt af The Institute of Technology Assessment (Austrian Academy of Sciences, Strohgassee 45/5, A-1030 Vienna) til alle partnere i SurPRISE konsortiet. Læs mere om projektet og partnerne på SurPRISE's webside: <http://surprise-project.eu/>

Informationen i dette informationshæfte stammer fra rapporter skrevet af SurPRISEs projektmedarbejdere, som har trukket på forskning og rapporter skrevet af forskere, politikere og teknologer fra hele verden.

> **Forfatter:** Kirstie Ball, The Open University; Maria Grazia Porcedda og Mathias Vermeulen, EUI; Elvira Santiago og Vincenzo Pavone, CSIC; Regina Berglez, IRKS; Eva Schlehahn, ULD; Márta Szénay, Medián.

> **Videnskabeligt rådgivningspanel:** Monica Areñas Ramiro, Colin Bennett, Gloria González Fuster, Ben Hayes, Majtényi László, Jean Marc Suchier, Nina Tranø, Ole Wæver

> **Layout:** Zsolt Bartha, Medián, baseret på det første hæfte forberedt af Peter Devine, David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University.

> **Billeder:** David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University

Side 11: Vision Systems, <http://www.vision-systems.co.nz/assets/Video-Analytics1.jpg>

Side 14: Mat Wellington, "Police Use QuadCopter – UK" March 23rd 2011,

<http://multirotornews.com/2011/03/23/police-use-quadcopter-uk>

Side 21: © iStockPhoto.com / Alexsl.

Side 23: Sensable City Lab, Massachusetts Institute of Technology.

Side 25: © KIVI NIRIA DV, 2011

> **SurPRISE sponsorer:** European Commission Framework 7 Programme

> **Denne publikation er tilgængelig på:** <http://surprise-project.eu>

> **Hvordan denne bog blev produceret:** Denne bog blev skrevet af Kirstie Ball i nært samarbejde med Fonden Teknologirådet, SurPRISE konsortiet og det videnskabelige rådgivningspanel. Bogen gennemgik fire interne revideringer samt en ekstern revidering og blev efterfølgende pilottestet af grupper i Danmark, Ungarn og England.

Projektpartnere

- > Institut für Technikfolgen-Abschätzung/Österreichische Akademie der Wissenschaften, Coordinator, Austria (ITA/OEAW)
- > Agencia de Protección de Datos de la Comunidad de Madrid*, Spain (APDCM)
- > Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain (CSIC)
- > Teknologirådet - The Danish Board of Technology Foundation, Denmark (DBT)
- > European University Institute, Italy (EUI)
- > Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
- > Median Opinion and Market Research Limited Company, Hungary (Median)
- > Teknologirådet - The Norwegian Board of Technology, Norway (NBT)
- > The Open University, United Kingdom (OU)
- > TA-SWISS/Akademien der Wissenschaften Schweiz, Switzerland (TA-SWISS)
- > Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Germany (ULD)

* APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Overvågning, privatliv og sikkerhed. Borgeres vurdering af sikkerhedsteknologier i Europa.

surprise
surveillance
privacy
security



